Karlsruhe Institute of Technology

KASTEL

Chosen-Ciphertext Secure Dual-Receiver Encryption in the Standard Model Based on Post-Quantum Assumptions

Laurin Benz Wasilij Beskorovajnov Sarai Eilebrecht Roland Gröll Maximilian Müller Jörn Müller-Quade |
16 April 2024

Preliminaries

Preliminaries

- Chosen-Ciphertext Security

Preliminaries

- Chosen-Ciphertext Security
- Standard Model

Preliminaries

- Chosen-Ciphertext Security
- Standard Model
- Post-Quantum Assumptions

Preliminaries

- Chosen-Ciphertext Security
- Standard Model
- Post-Quantum Assumptions
- Dual-Receiver Encryption

Preliminaries

- Chosen-Ciphertext Security
- Standard Model
- Post-Quantum Assumptions
- $\rightarrow$**Dual-Receiver Encryption**

Preliminaries

- $\rightarrow$ **Chosen-Ciphertext-Security**
- Standard Model
- Post-Quantum Assumptions
- $\rightarrow$**Dual-Receiver Encryption**

Dual-Receiver Encryption

Dual-Receiver Encryption

- Want to encrypt a message to **two** recipients

Dual-Receiver Encryption

- Want to encrypt a message to **two** recipients
- Special case of Broadcast encryption

Dual-Receiver Encryption

Karlsruhe Institute of Technology

- Want to encrypt a message to **two** recipients
- Special case of Broadcast encryption

Definition of DRE

- $\texttt{gen}(1^\lambda)$: takes security parameter, outputs one public/secret key pair (pk, sk)
- $\texttt{enc}(pk^R, pk^S, m)$: takes two (independent) public keys and a message, outputs ciphertext c
- $\texttt{dec}(sk^i, pk^R, pk^S, c)$: takes one secret key, both public keys and a ciphertext c, outputs message m^i

Dual-Receiver Encryption

Karlsruhe Institute of Technology

Naive implementation

Dual-Receiver Encryption

Naive implementation

- Take any PKE-scheme $PK = (\mathtt{gen}_{PK}, \mathtt{enc}_{PK}, \mathtt{dec}_{PK})$

Dual-Receiver Encryption

Naive implementation

- Take any PKE-scheme $PK = (\mathtt{gen}_{PK}, \mathtt{enc}_{PK}, \mathtt{dec}_{PK})$
- Define DRE-scheme $DR = (\mathtt{gen}_{DR}, \mathtt{enc}_{DR}, \mathtt{dec}_{DR})$ by

Dual-Receiver Encryption

Naive implementation

- Take any PKE-scheme $PK = (\mathtt{gen}_{PK}, \mathtt{enc}_{PK}, \mathtt{dec}_{PK})$
- Define DRE-scheme $DR = (\mathtt{gen}_{DR}, \mathtt{enc}_{DR}, \mathtt{dec}_{DR})$ by
  - $\mathtt{gen}_{DR} = \mathtt{gen}_{PK}$

Dual-Receiver Encryption

Naive implementation

- Take any PKE-scheme $PK = (\mathtt{gen}_{PK}, \mathtt{enc}_{PK}, \mathtt{dec}_{PK})$
- Define DRE-scheme $DR = (\mathtt{gen}_{DR}, \mathtt{enc}_{DR}, \mathtt{dec}_{DR})$ by
  - $\mathtt{gen}_{DR} = \mathtt{gen}_{PK}$
  - $\mathtt{enc}_{DR}(pk^R, pk^S, m) = (\mathtt{enc}_{PK}(pk^R, m), \mathtt{enc}_{PK}(pk^S, m))$

Dual-Receiver Encryption

Karlsruhe Institute of Technology

Naive implementation

- Take any PKE-scheme $PK = (\mathtt{gen}_{PK}, \mathtt{enc}_{PK}, \mathtt{dec}_{PK})$
- Define DRE-scheme $DR = (\mathtt{gen}_{DR}, \mathtt{enc}_{DR}, \mathtt{dec}_{DR})$ by
  - $\mathtt{gen}_{DR} = \mathtt{gen}_{PK}$
  - $\mathtt{enc}_{DR}(pk^R, pk^S, m) = (\mathtt{enc}_{PK}(pk^R, m), \mathtt{enc}_{PK}(pk^S, m)) = (c^R, c^S)$

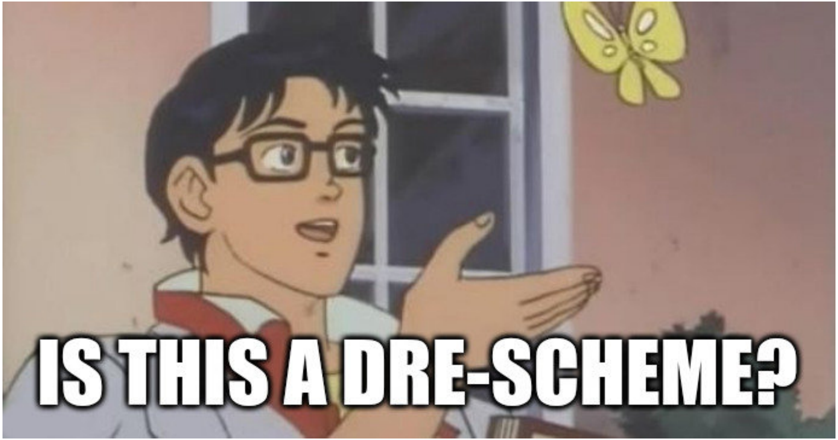
Dual-Receiver Encryption

Karlsruhe Institute of Technology

Naive implementation

- Take any PKE-scheme $PK = (\mathtt{gen}_{PK}, \mathtt{enc}_{PK}, \mathtt{dec}_{PK})$
- Define DRE-scheme $DR = (\mathtt{gen}_{DR}, \mathtt{enc}_{DR}, \mathtt{dec}_{DR})$ by
  - $\mathtt{gen}_{DR} = \mathtt{gen}_{PK}$
  - $\mathtt{enc}_{DR}(pk^R, pk^S, m) = (\mathtt{enc}_{PK}(pk^R, m), \mathtt{enc}_{PK}(pk^S, m)) = (c^R, c^S)$
  - $\mathtt{dec}_{DR}(sk^i, pk^R, pk^S, c) = \mathtt{dec}_{PK}(sk^i, c^i)$

Dual-Receiver Encryption - soundness



Dual-Receiver Encryption - soundness

- Yes!

Dual-Receiver Encryption - soundness

- Yes!
- ...but its not very useful

Dual-Receiver Encryption - soundness

- Yes!
- ...but its not very useful
- Want $\texttt{dec}(sk^R, pk^R, pk^S, c) = \texttt{dec}(sk^S, pk^R, pk^S, c)$

Dual-Receiver Encryption - soundness

- Yes!
- ...but its not very useful
- Want $\texttt{dec}(sk^R, pk^R, pk^S, c) = \texttt{dec}(sk^S, pk^R, pk^S, c)$ even for malicious ciphertexts

Dual-Receiver Encryption - soundness

- Yes!
- ...but its not very useful
- Want $\texttt{dec}(sk^R, pk^R, pk^S, c) = \texttt{dec}(sk^S, pk^R, pk^S, c)$ even for malicious ciphertexts
- This is called **soundness**

Dual-Receiver Encryption - soundness

- Yes!
- ...but its not very useful
- Want $\texttt{dec}(sk^R, pk^R, pk^S, c) = \texttt{dec}(sk^S, pk^R, pk^S, c)$ even for malicious ciphertexts
- This is called **soundness**
- Formal definition as usual through a game

Dual-Receiver Encryption - CCA2

Dual-Receiver Encryption - CCA2

- $\mathcal{A}$ gets **two** public keys

Dual-Receiver Encryption - CCA2

- $\mathcal{A}$ gets **two** public keys
- Slightly different decryption oracle $\mathcal{O}$

Dual-Receiver Encryption - CCA2

$$\xrightarrow{(\mathbf{c}, pk^{R'})}$$

$$\begin{aligned}&\textbf{if } R' \in \{S, R\} \wedge \mathbf{c} \neq \mathbf{c}^* \\ &\ \textbf{then } \mathbf{m} = \mathtt{dec}(sk^{R'}, pk^R, pk^S, \mathbf{c}) \\ &\textbf{else } \mathbf{m} = \perp\end{aligned}$$

$$\xleftarrow{\mathbf{m}'}$$

- $\mathcal{A}$ gets **two** public keys
- Slightly different decryption oracle $\mathcal{O}$

Dual-Receiver Encryption - CCA2

Karlsruhe Institute of Technology

$$\xrightarrow{(\mathbf{c}, pk^{R'})}$$

$$\begin{aligned}&\textbf{if } R' \in \{S, R\} \wedge \mathbf{c} \neq \mathbf{c}^* \\ &\textbf{then } \mathbf{m} = \mathtt{dec}(sk^{R'}, pk^R, pk^S, \mathbf{c}) \\ &\textbf{else } \mathbf{m} = \perp\end{aligned}$$

$$\xleftarrow{\mathbf{m}'}$$

- $\mathcal{A}$ gets **two** public keys
- Slightly different decryption oracle $\mathcal{O}$
- With soundness this collapses to the PKE CCA definition

Dual-Receiver Encryption - Applications of sound DRE

Dual-Receiver Encryption - Applications of sound DRE

- Plaintext Awareness via Key Registration

Dual-Receiver Encryption - Applications of sound DRE

Karlsruhe Institute of Technology

- Plaintext Awareness via Key Registration
  - Dolev-Yao model for automated theorem provers

Dual-Receiver Encryption - Applications of sound DRE

- Plaintext Awareness via Key Registration
  - Dolev-Yao model for automated theorem provers
- Key Exchange with Incriminating Abort

Dual-Receiver Encryption - Applications of sound DRE

- Plaintext Awareness via Key Registration
  - Dolev-Yao model for automated theorem provers
- Key Exchange with Incriminating Abort
- PKE with Non-Interactive Opening

Dual-Receiver Encryption - Applications of sound DRE

- Plaintext Awareness via Key Registration
  - Dolev-Yao model for automated theorem provers
- Key Exchange with Incriminating Abort
- PKE with Non-Interactive Opening
- ... and many more

Related Work

Related Work

- There already exist:

Related Work

- There already exist:
  - Sound PQ DRE schemes

Related Work

- There already exist:
  - Sound PQ DRE schemes (which are not CCA)

Related Work

- There already exist:
  - Sound PQ DRE schemes (which are not CCA)
  - Sound CCA DRE schemes

Related Work

- There already exist:
  - Sound PQ DRE schemes (which are not CCA)
  - Sound CCA DRE schemes (which are not PQ)

Related Work

- There already exist:
  - Sound PQ DRE schemes (which are not CCA)
  - Sound CCA DRE schemes (which are not PQ)
  - PQ CCA DRE schemes

Related Work

- There already exist:
  - Sound PQ DRE schemes (which are not CCA)
  - Sound CCA DRE schemes (which are not PQ)
  - PQ CCA DRE schemes (which are not sound)

Related Work

- There already exist:
  - Sound PQ DRE schemes (which are not CCA)
  - Sound CCA DRE schemes (which are not PQ)
  - PQ CCA DRE schemes (which are not sound)
- ... but no sound CCA PQ DRE scheme

Our contributions

Our contributions

- Showing that no previously known PQ CCA DRE scheme satisfies soundness by constructing malicious ciphertexts

Our contributions

- Showing that no previously known PQ CCA DRE scheme satisfies soundness by constructing malicious ciphertexts
- Construction of two efficient PQ CCA DRE schemes with soundness

Our contributions

- Showing that no previously known PQ CCA DRE scheme satisfies soundness by constructing malicious ciphertexts
- Construction of two efficient PQ CCA DRE schemes with soundness
- ...one based on LWE, one based on LPN

Our contributions

Karlsruhe Institute of Technology

- Showing that no previously known PQ CCA DRE scheme satisfies soundness by constructing malicious ciphertexts
- Construction of two efficient PQ CCA DRE schemes with soundness
- ...one based on LWE, one based on LPN
- First DRE scheme based on LPN

Our contributions

- Showing that no previously known PQ CCA DRE scheme satisfies soundness by constructing malicious ciphertexts
- Construction of two efficient PQ CCA DRE schemes with soundness
- ...one based on LWE, one based on LPN
- First DRE scheme based on LPN
- Inspired by Kiltz, Masny, and Pietrzak (2014)

Our contributions

- Showing that no previously known PQ CCA DRE scheme satisfies soundness by constructing malicious ciphertexts
- Construction of two efficient PQ CCA DRE schemes with soundness
- ...one based on LWE, one based on LPN
- First DRE scheme based on LPN
- Inspired by Kiltz, Masny, and Pietrzak (2014)
- Both use the hybrid encryption paradigm

Our contributions - LPN

Hybrid encryption

$$\mathbf{s} \leftarrow_{\$} \{0,1\}^n$$

$$(dk, mk) := \mathtt{KDF}(\mathbf{s})$$

$$\phi := \mathtt{SKE.enc}(dk, \mathbf{M})$$

$$\sigma := \mathtt{MAC.sign}(mk, (\mathbf{c}_0, \mathbf{c}_1, \phi))$$

Our contributions - LPN
Hybrid encryption

$$\mathbf{s} \leftarrow_{\$} \{0,1\}^n$$
$$(dk, mk) := \mathtt{KDF}(\mathbf{s})$$
$$\phi := \mathtt{SKE.enc}(dk, \mathbf{M})$$
$$\sigma := \mathtt{MAC.sign}(mk, (\mathbf{c}_0, \mathbf{c}_1, \phi))$$

- The secret *s* of the asymmetric part is only used to derive MAC and SKE keys

Our contributions - LPN
Hybrid encryption

$$\mathbf{s} \leftarrow_{\$} \{0,1\}^n$$
$$(dk, mk) := \mathtt{KDF}(\mathbf{s})$$
$$\phi := \mathtt{SKE.enc}(dk, \mathbf{M})$$
$$\sigma := \mathtt{MAC.sign}(mk, (\mathbf{c}_0, \mathbf{c}_1, \phi))$$

- The secret *s* of the asymmetric part is only used to derive MAC and SKE keys
- The encryption is then symmetric

Our contributions - LPN

Hybrid encryption

$$
\begin{aligned}
3:&\quad \mathbf{s} \leftarrow\!\!\$\ \{0,1\}^n \\
4:&\quad (dk, mk) := \mathtt{KDF}(\mathbf{s}) \\
9:&\quad \phi := \mathtt{SKE.enc}(dk, \mathbf{M}) \\
10:&\quad \sigma := \mathtt{MAC.sign}(mk, (\mathbf{c}_0, \mathbf{c}_1, \phi))
\end{aligned}
$$

- The secret *s* of the asymmetric part is only used to derive MAC and SKE keys
- The encryption is then symmetric
- Makes encryption smaller and faster for larger messages

Our contributions - LPN
Soundness

$$\textbf{if } \left\| \mathbf{c}_0^R - \mathbf{s}^\top \mathbf{A}^R \right\|_w > \beta \text{ output } \bot$$

$$\textbf{if } \left\| \mathbf{c}_0^S - \mathbf{s}^\top \mathbf{A}^S \right\|_w > \beta \text{ output } \bot$$

$$\textbf{if } \left\| \mathbf{c}_1^R - \mathbf{s}^\top (\mathbf{A}_1^R + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) \right\|_w > \frac{\alpha m}{2}$$

$$\textbf{if } \left\| \mathbf{c}_1^S - \mathbf{s}^\top (\mathbf{A}_1^S + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) \right\|_w > \frac{\alpha m}{2}$$

Our contributions - LPN

Soundness

$$\textbf{if } \left\| \mathbf{c}_0^R - \mathbf{s}^\top \mathbf{A}^R \right\|_w > \beta \text{ output } \perp$$

$$\textbf{if } \left\| \mathbf{c}_0^S - \mathbf{s}^\top \mathbf{A}^S \right\|_w > \beta \text{ output } \perp$$

$$\textbf{if } \left\| \mathbf{c}_1^R - \mathbf{s}^\top (\mathbf{A}_1^R + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) \right\|_w > \frac{\alpha m}{2}$$

$$\textbf{if } \left\| \mathbf{c}_1^S - \mathbf{s}^\top (\mathbf{A}_1^S + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) \right\|_w > \frac{\alpha m}{2}$$

- Consistency check can be done with only the public keys

Our contributions - LPN
Soundness

$$7: \quad \textbf{if } \left\| \mathbf{c}_0^R - \mathbf{s}^\top \mathbf{A}^R \right\|_w > \beta \text{ output } \bot$$

$$8: \quad \textbf{if } \left\| \mathbf{c}_0^S - \mathbf{s}^\top \mathbf{A}^S \right\|_w > \beta \text{ output } \bot$$

$$9: \quad \textbf{if } \left\| \mathbf{c}_1^R - \mathbf{s}^\top (\mathbf{A}_1^R + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) \right\|_w > \frac{\alpha m}{2}$$

$$10: \quad \textbf{if } \left\| \mathbf{c}_1^S - \mathbf{s}^\top (\mathbf{A}_1^S + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) \right\|_w > \frac{\alpha m}{2}$$

- Consistency check can be done with only the public keys
- “Soundness check” nearly for free

Our contributions - LPN

$$6 : \mathbf{c}_0 = (\mathbf{s}^\top \mathbf{A}^R + \mathbf{e}^R, \mathbf{s}^\top \mathbf{A}^S + \mathbf{e}^S)$$

$$8 : \mathbf{c}_1 = \big(\mathbf{s}^\top (\mathbf{A}_1^R + \mathsf{FRD}(\mathsf{H}(\mathbf{c}_0))\mathbf{G}) + (\mathbf{e}^R)^\top \mathbf{T}^R, \\ \mathbf{s}^\top (\mathbf{A}_1^S + \mathsf{FRD}(\mathsf{H}(\mathbf{c}_0))\mathbf{G}) + (\mathbf{e}^S)^\top \mathbf{T}^S\big)$$

Our contributions - LPN

$$6 : \mathbf{c}_0 = (\mathbf{s}^\top \mathbf{A}^R + \mathbf{e}^R, \mathbf{s}^\top \mathbf{A}^S + \mathbf{e}^S)$$

$$\begin{aligned} 8 : \mathbf{c}_1 = \big(&\mathbf{s}^\top (\mathbf{A}_1^R + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) + (\mathbf{e}^R)^\top \mathbf{T}^R, \\ &\mathbf{s}^\top (\mathbf{A}_1^S + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) + (\mathbf{e}^S)^\top \mathbf{T}^S\big) \end{aligned}$$

- Low overhead compared to the LPN PKE

Our contributions - LPN

$$6 : \mathbf{c}_0 = (\mathbf{s}^\top \mathbf{A}^R + \mathbf{e}^R, \mathbf{s}^\top \mathbf{A}^S + \mathbf{e}^S)$$

$$8 : \mathbf{c}_1 = \big(\mathbf{s}^\top (\mathbf{A}_1^R + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) + (\mathbf{e}^R)^\top \mathbf{T}^R, \\ \mathbf{s}^\top (\mathbf{A}_1^S + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) + (\mathbf{e}^S)^\top \mathbf{T}^S\big)$$

- Low overhead compared to the LPN PKE
- $(\mathbf{c}^R, \mathbf{c}^S)$ naturally acts as a “double trapdoor”, allowing the simulation of the decryption oracle in the CCA proof

Our contributions - LPN

$$6: \mathbf{c}_0 = (\mathbf{s}^\top \mathbf{A}^R + \mathbf{e}^R, \mathbf{s}^\top \mathbf{A}^S + \mathbf{e}^S)$$

$$8: \mathbf{c}_1 = (\mathbf{s}^\top (\mathbf{A}_1^R + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) + (\mathbf{e}^R)^\top \mathbf{T}^R, \mathbf{s}^\top (\mathbf{A}_1^S + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) + (\mathbf{e}^S)^\top \mathbf{T}^S)$$

- Low overhead compared to the LPN PKE
- $(\mathbf{c}^R, \mathbf{c}^S)$ naturally acts as a "double trapdoor", allowing the simulation of the decryption oracle in the CCA proof

Our contributions - LPN

$$6 : \mathbf{c}_0 = (\mathbf{s}^\top \mathbf{A}^R + \mathbf{e}^R, \mathbf{s}^\top \mathbf{A}^S + \mathbf{e}^S)$$

$$8 : \mathbf{c}_1 = (\mathbf{s}^\top (\mathbf{A}_1^R + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) + (\mathbf{e}^R)^\top \mathbf{T}^R, \mathbf{s}^\top (\mathbf{A}_1^S + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) + (\mathbf{e}^S)^\top \mathbf{T}^S)$$

- Low overhead compared to the LPN PKE
- $(\mathbf{c}^R, \mathbf{c}^S)$ naturally acts as a “double trapdoor”, allowing the simulation of the decryption oracle in the CCA proof

Our contributions - LPN

Karlsruhe Institute of Technology

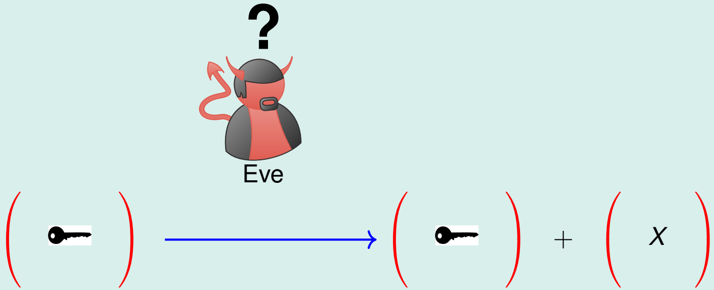
“Double trapdoor”

Need to change public key $= A_1^R$ from $A_1^R = A^R \cdot R^R$ to $A_1^R = A^R \cdot R^R + X$ for A^R and X known matrices

Our contributions - LPN

“Double trapdoor”

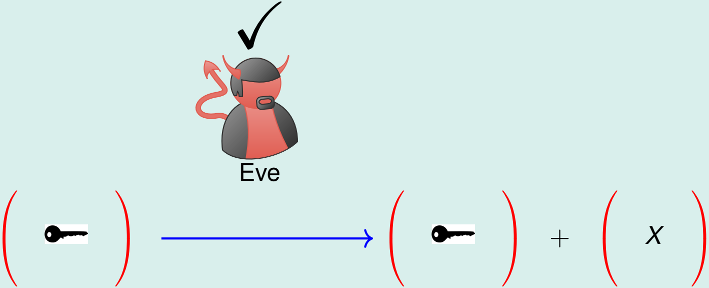
Need to change public key  $= A_1^R$ from $A_1^R = A^R \cdot R^R$ to $A_1^R = A^R \cdot R^R + X$ for A^R and X known matrices



Our contributions - LPN

“Double trapdoor”

Need to change public key  $= A_1^R$ from $A_1^R = A^R \cdot R^R$ to $A_1^R = A^R \cdot R^R + X$ for A^R and X known matrices



Our contributions - LPN

“Double trapdoor”

Need to change public key $= A_1^R$ from $A_1^R = A^R \cdot R^R$ to $A_1^R = A^R \cdot R^R + X$ for A^R and X known matrices

$$\begin{pmatrix} U \end{pmatrix} \longrightarrow \begin{pmatrix} U \end{pmatrix} + \begin{pmatrix} X \end{pmatrix}$$

Our contributions - LPN

Karlsruhe Institute of Technology

"Double trapdoor"

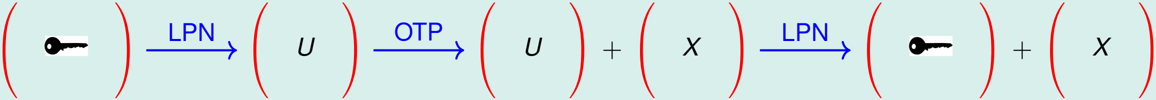
Need to change public key $= A_1^R$ from $A_1^R = A^R \cdot R^R$ to $A_1^R = A^R \cdot R^R + X$ for A^R and X known matrices

$$\begin{pmatrix} U \end{pmatrix} \longrightarrow \begin{pmatrix} U \end{pmatrix} + \begin{pmatrix} X \end{pmatrix}$$

Our contributions - LPN

"Double trapdoor"

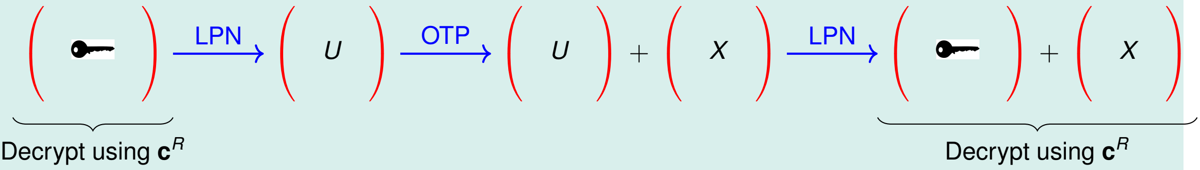
Need to change public key  $= A_1^R$ from $A_1^R = A^R \cdot R^R$ to $A_1^R = A^R \cdot R^R + X$ for A^R and X known matrices



Our contributions - LPN

"Double trapdoor"

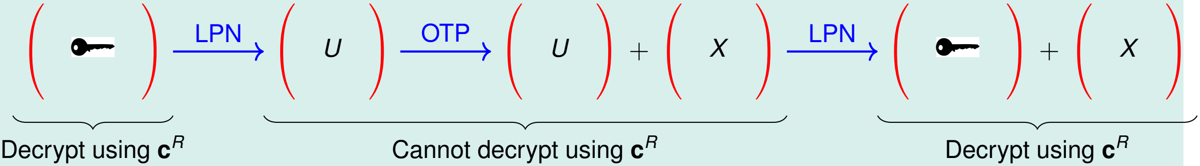
Need to change public key  $= A_1^R$ from $A_1^R = A^R \cdot R^R$ to $A_1^R = A^R \cdot R^R + X$ for A^R and X known matrices



Our contributions - LPN

“Double trapdoor”

Need to change public key $= A_1^R$ from $A_1^R = A^R \cdot R^R$ to $A_1^R = A^R \cdot R^R + X$ for A^R and X known matrices



Our contributions - LPN

Karlsruhe Institute of Technology

“Double trapdoor”

Need to change public key  $= A_1^R$ from $A_1^R = A^R \cdot R^R$ to $A_1^R = A^R \cdot R^R + X$ for A^R and X known matrices

$\Big($  $\Big) \xrightarrow{\text{LPN}} \Big(U \Big) \xrightarrow{\text{OTP}} \Big(U \Big) + \Big(X \Big) \xrightarrow{\text{LPN}} \Big($  $\Big) + \Big(X \Big)$

Decrypt using $\mathbf{c}^R$ — Can decrypt using $\mathbf{c}^S$ (soundness!) — Decrypt using $\mathbf{c}^R$

Our contributions - LWE

Our contributions - LWE

- Similar construction and soundness check

Our contributions - LWE

- Similar construction and soundness check
- Proof easier thanks to A_1 being statistical indistinguishable from randomness

Our contributions - LWE

- Similar construction and soundness check
- Proof easier thanks to A_1 being statistical indistinguishable from randomness
- Bigger ciphertexts, but smaller keys

Summary

Summary

- Known Post-Quantum CCA secure Dual-Receiver Encryption schemes are not sound

Summary

- Known Post-Quantum CCA secure Dual-Receiver Encryption schemes are not sound
- First sound Post-Quantum CCA secure Dual-Receiver Encryption schemes in the standard model

Summary

- Known Post-Quantum CCA secure Dual-Receiver Encryption schemes are not sound
- First sound Post-Quantum CCA secure Dual-Receiver Encryption schemes in the standard model
- Known primitives, allows relatively easy implementation

Summary

Karlsruhe Institute of Technology

- Known Post-Quantum CCA secure Dual-Receiver Encryption schemes are not sound
- First sound Post-Quantum CCA secure Dual-Receiver Encryption schemes in the standard model
- Known primitives, allows relatively easy implementation
- Room for optimizations like R-LWE, compression techniques etc

Summary

Thank you for your attention. Any questions?

Sizes of the constructions

Karlsruhe Institute of Technology

Table: Sizes of $\text{PKE}_{\texttt{LWE-DRE}}$

	$\|pk\|$ for one party	$\|sk\|$	$\|c\|$
Generic sizes	$\lceil \log q \rceil \cdot (n \cdot (m + \bar{m}))$	$\lceil \log q \rceil \cdot (m \cdot \bar{m})$	$\lceil \log q \rceil \cdot (2 \cdot (m + \bar{m}))$
Exact sizes	61.45MB	58.49MB	91.45kB

Table: Sizes of $\text{PKE}_{\texttt{LPN-DRE}}$

	$\|pk\|$ for one party	$\|sk\|$	$\|c\|$
Generic sizes	$2 \cdot n \cdot m$	m^2	$4 \cdot m$
Exact sizes	351.13MB	351.13MB	26.5kB

Our contributions - LPN

$\mathtt{gen}(1^\lambda)$

$\mathbf{A} \leftarrow\!\!\$\ \mathbb{Z}_2^{n\times m}, \mathbf{R} \leftarrow \mathrm{Ber}_p^{m\times m}$

$\mathbf{A}_1 = \mathbf{A}\cdot\mathbf{R}$

$\mathbf{return}\ (pk, sk) := ((\mathbf{A}, \mathbf{A}_1), \mathbf{R})$

$\mathtt{enc}(pk^R, pk^S, \mathbf{M})$

$\text{parse } pk^R = (\mathbf{A}^R, \mathbf{A}_1^R)$

$\text{parse } pk^S = (\mathbf{A}^S, \mathbf{A}_1^S)$

$\mathbf{s} \leftarrow\!\!\$\ \{0,1\}^n$

$(dk, mk) := \mathtt{KDF}(\mathbf{s})$

$\mathbf{e}^R, \mathbf{e}^S \leftarrow \mathrm{Ber}_p^m$

$\mathbf{c}_0 = (\mathbf{s}^\top\mathbf{A}^R + \mathbf{e}^R, \mathbf{s}^\top\mathbf{A}^S + \mathbf{e}^S)$

$\mathbf{T}^R, \mathbf{T}^S \leftarrow \mathrm{Ber}_p^{m\times m}$

$\mathbf{c}_1 = \big(\mathbf{s}^\top(\mathbf{A}_1^R + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) + (\mathbf{e}^R)^\top\mathbf{T}^R,$
$\mathbf{s}^\top(\mathbf{A}_1^S + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G}) + (\mathbf{e}^S)^\top\mathbf{T}^S\big)$

$\phi := \mathtt{SKE.enc}(dk, \mathbf{M})$

$\sigma := \mathtt{MAC.sign}(mk, (\mathbf{c}_0, \mathbf{c}_1, \phi))$

$\mathbf{return}\ \mathbf{c} = (\mathbf{c}_0, \mathbf{c}_1, \phi, \sigma)$

$\mathtt{dec}(sk^R, pk^R, pk^S, \mathbf{C})$

$\text{parse } pk^R = (\mathbf{A}^R, \mathbf{A}_1^R)$

$\text{parse } pk^S = (\mathbf{A}^S, \mathbf{A}_1^S)$

$\text{parse } sk^R = (\mathbf{R}^R)$

$\text{parse } \mathbf{C} = (\mathbf{c}_0^R, \mathbf{c}_0^S, \mathbf{c}_1^R, \mathbf{c}_1^S, \phi, \sigma)$

$\mathbf{c}_t^R := \mathbf{c}_1^R - \mathbf{c}_0^R\mathbf{R}^R$

$\mathbf{s} := \mathtt{decode}_{\mathbf{G}}\left(\mathbf{c}_t^R\right) \cdot \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))^{-1}$

$\textbf{if } \left\|\mathbf{c}_0^R - \mathbf{s}^\top\mathbf{A}^R\right\|_w > \beta \text{ output } \perp$

$\textbf{if } \left\|\mathbf{c}_0^S - \mathbf{s}^\top\mathbf{A}^S\right\|_w > \beta \text{ output } \perp$

$\textbf{if } \left\|\mathbf{c}_1^R - \mathbf{s}^\top(\mathbf{A}_1^R + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G})\right\|_w > \frac{\alpha m}{2}$

$\textbf{if } \left\|\mathbf{c}_1^S - \mathbf{s}^\top(\mathbf{A}_1^S + \mathtt{FRD}(\mathtt{H}(\mathbf{c}_0))\mathbf{G})\right\|_w > \frac{\alpha m}{2}$

$(dk, mk) = \mathtt{KDF}(\mathbf{s})$

$\textbf{if } 1 == \mathtt{MAC.Vfy}(mk, (\mathbf{c}_0, \mathbf{c}_1, \phi), \sigma)$

$\mathbf{return}\ \mathbf{M} = \mathtt{SKE.dec}(dk, \phi)$

$\textbf{else return}\ \mathbf{M} = \perp$

References

[1] Eike Kiltz, Daniel Masny, and Krzysztof Pietrzak. “Simple Chosen-Ciphertext Security from Low-Noise LPN”. In: *PKC 2014*. Ed. by Hugo Krawczyk. Vol. 8383. LNCS. Springer, Heidelberg, Mar. 2014, pp. 1–18. DOI: 10.1007/978-3-642-54631-0_1.