Decoding problems with hints and applications to multi-receiver code-based encryption schemes

Thomas Debris-Alazard[1], **Victor Dyseryn**[2], Duong Hieu Phan[2]

[1]Inria and LIX, Institut Polytechnique de Paris, École Polytechnique, Palaiseau, France
[2]Institut Polytechnique de Paris, Télécom Paris, Palaiseau, France

CBCrypto 2026 - May 8

Outline

Outline

Decoding Problem

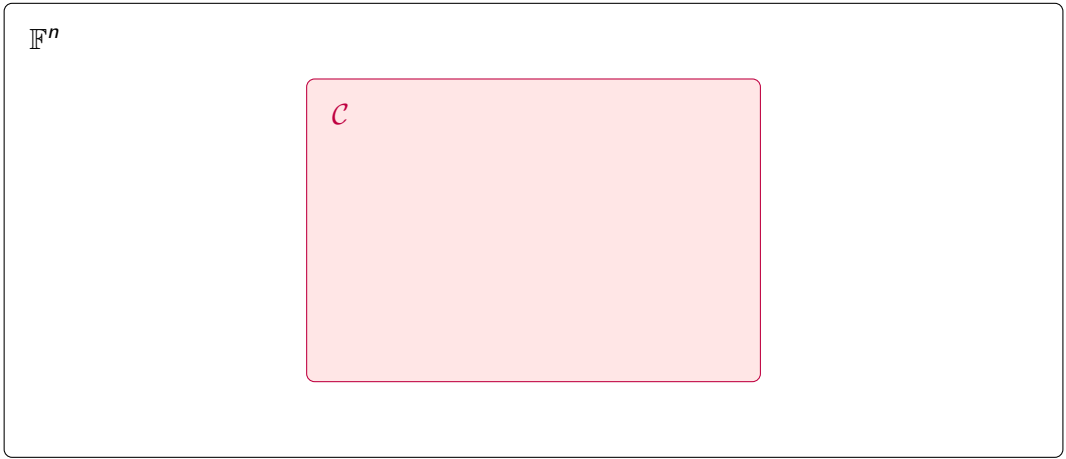
Distinguish between distributions

$$(\boldsymbol{G}, \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}) \quad \text{and} \quad (\boldsymbol{G}, \boldsymbol{u} + \boldsymbol{e})$$

for

- $\boldsymbol{G} \hookleftarrow \mathbb{F}^{k \times n}$
- $\boldsymbol{e} \hookleftarrow \mathcal{B}er(\omega)^n, \boldsymbol{x} \hookleftarrow \mathbb{F}^k$
- $\boldsymbol{u} \hookleftarrow \mathbb{F}^n$

Decoding Problem



Decoding Problem with hint

Distinguish between distributions

$$(\boldsymbol{v}, \boldsymbol{G}, \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}) \quad \text{and} \quad (\boldsymbol{v}, \boldsymbol{G}, \boldsymbol{u} + \boldsymbol{e})$$

for

- $\boldsymbol{v} \hookleftarrow \mathcal{B}er(\sigma)^n, \boldsymbol{G} \hookleftarrow \{\boldsymbol{M} \in \mathbb{F}^{k \times n} \mid \boldsymbol{M}\boldsymbol{v}^T = \boldsymbol{0}\}$
- $\boldsymbol{e} \hookleftarrow \mathcal{B}er(\omega)^n, \boldsymbol{x} \hookleftarrow \mathbb{F}^k$
- $\boldsymbol{u} \hookleftarrow \mathbb{F}^n$

Decoding Problem with hint

Distinguish between distributions

$$(\boldsymbol{v}, \boldsymbol{G}, \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}) \quad \text{and} \quad (\boldsymbol{v}, \boldsymbol{G}, \boldsymbol{u} + \boldsymbol{e})$$

for

- $\boldsymbol{v} \hookleftarrow \mathcal{B}er(\sigma)^n, \boldsymbol{G} \hookleftarrow \{\boldsymbol{M} \in \mathbb{F}^{k \times n} \mid \boldsymbol{M}\boldsymbol{v}^T = \boldsymbol{0}\}$
- $\boldsymbol{e} \hookleftarrow \mathcal{B}er(\omega)^n, \boldsymbol{x} \hookleftarrow \mathbb{F}^k$
- $\boldsymbol{u} \hookleftarrow \langle \boldsymbol{v} \rangle^{\perp}$

Decoding Problem with ℓ hints

Distinguish between distributions

$$(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell, \boldsymbol{G}, \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}) \quad \text{and} \quad (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell, \boldsymbol{G}, \boldsymbol{u} + \boldsymbol{e})$$

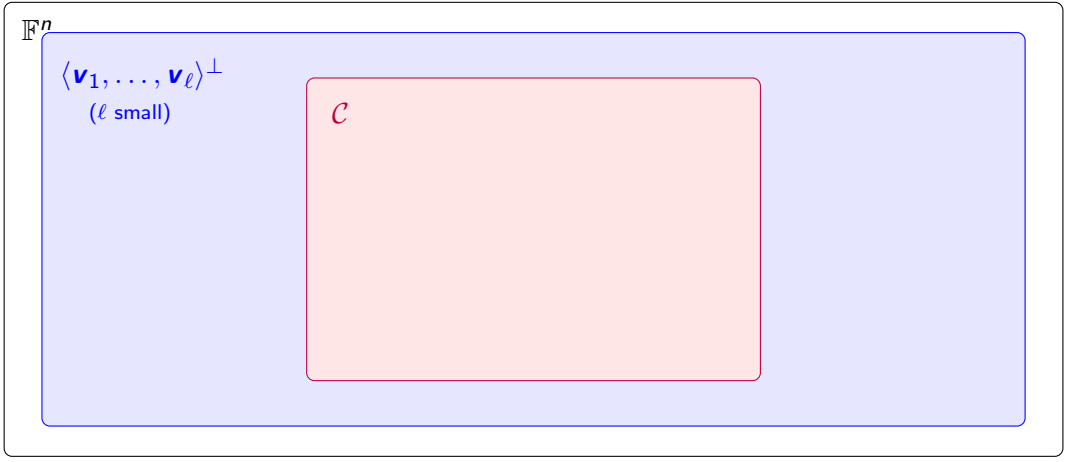
for

- $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell \hookleftarrow \mathcal{B}er(\sigma)^n, \boldsymbol{G} \hookleftarrow \{\boldsymbol{M} \in \mathbb{F}^{k \times n} \mid \boldsymbol{M}\boldsymbol{v}_i^T = \boldsymbol{0} \text{ forall } i \in [1, \ell]\}$
- $\boldsymbol{e} \hookleftarrow \mathcal{B}er(\omega)^n, \boldsymbol{x} \hookleftarrow \mathbb{F}^k$
- $\boldsymbol{u} \hookleftarrow \langle \boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell \rangle^\perp$

Analog to k-LWE problem [LPSS14]

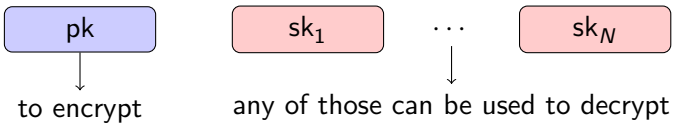
[LPSS14]: Ling, Phan, Stehlé, and Steinfeld. Hardness of k-LWE and applications in traitor tracing. (CRYPTO'14)

Decoding Problem with ℓ hints



Outline

What is a Multi-receiver PKE?

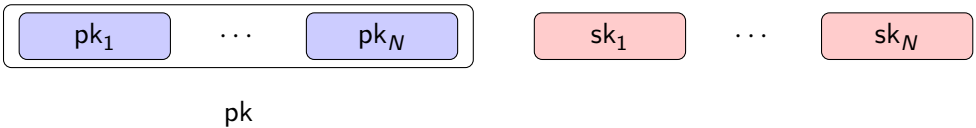


- $\mathsf{KeyGen}(1^\lambda, 1^N) \to (\mathsf{pk}, (\mathsf{sk}_1, \ldots, \mathsf{sk}_N))$

Properties:

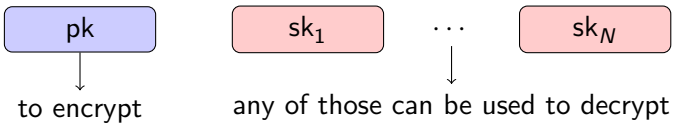
- Correctness: $\mathsf{Dec}\big(\mathsf{Enc}(m, \mathsf{pk}), \mathsf{sk}_i\big) = m$ for any $i \in [1, N]$
- IND-CPA security
- Compactness: $|\mathsf{ct}|, |\mathsf{pk}| \ll \lambda N$

Why compactness?



Not compact!

What is a Multi-receiver PKE?



- $\mathsf{KeyGen}(1^\lambda, 1^N) \to (\mathsf{pk}, (\mathsf{sk}_1, \ldots, \mathsf{sk}_N))$

Properties:

- Correctness: $\mathsf{Dec}\big(\mathsf{Enc}(m, \mathsf{pk}), \mathsf{sk}_i\big) = m$ for any $i \in [1, N]$
- IND-CPA security
- Compactness: $|\mathsf{ct}|, |\mathsf{pk}| \ll \lambda N$

A compact but trivial solution

- MultiPKE.KeyGen$(1^\lambda, 1^N)$:
  $(\mathsf{pk}, \mathsf{sk}) \leftarrow$ PKE.KeyGen(1^λ)
  Output $(\mathsf{pk}, (\mathsf{sk}, \ldots, \mathsf{sk}))$
- MultiPKE.Enc(m, pk) :
  Output $\mathsf{ct} =$ PKE.Enc(m, pk)
- MultiPKE.Dec$(\mathsf{ct}, \mathsf{sk})$:
  Output $m =$ PKE.Dec$(\mathsf{ct}, \mathsf{sk})$

We need more than bare IND-CPA security.
Force some difference between secret keys.

Multi-receiver PKE with revocation

- $\mathsf{MultiPKE.KeyGen}(1^\lambda, 1^N) \to (\mathsf{pk}, (\mathsf{sk}_1, \ldots, \mathsf{sk}_N))$
- $\mathsf{MultiPKE.Enc}\Big(m, \mathsf{pk}, \underbrace{(\mathsf{sk}_i)_{i\in\mathcal{C}}}_{\text{revoked users}}\Big) \to \mathsf{ct}$ (for a set $\mathcal{C} \subset [1, N]$)
- $\mathsf{MultiPKE.Dec}(\mathsf{ct}, \mathsf{sk}) \to m$

Properties:

- Correctness: $\mathsf{MultiPKE.Dec}\Big[\mathsf{MultiPKE.Enc}\Big(m, \mathsf{pk}, (\mathsf{sk}_i)_{i\in\mathcal{C}}\Big), \mathsf{sk}_j\Big] = m$ for any $j \in [1, N]\backslash\mathcal{C}$
- IND-CPA security with revocation
- Compactness: $|\mathsf{ct}|, |\mathsf{pk}| \ll \lambda N$

Alekhnovich PKE (1-bit scheme)

- PKE.KeyGen(1^λ) :

  $\boldsymbol{e} \hookleftarrow \mathcal{B}er(\sigma)^n$

  $\boldsymbol{G} \hookleftarrow \{\boldsymbol{M} \in \mathbb{F}^{k \times n} \mid \boldsymbol{M}\boldsymbol{e}^T = \boldsymbol{0}\}$

  Output $\mathsf{pk} = \boldsymbol{G}$ and $\mathsf{sk} = \boldsymbol{e}$

- PKE.Enc$(m \in \{0,1\}, \mathsf{pk} = \boldsymbol{G})$:

  $\boldsymbol{e}' \hookleftarrow \mathcal{B}er(\sigma)^n, \boldsymbol{x} \hookleftarrow \mathbb{F}^k$

  Output $\mathsf{ct} = \underset{(\text{if } m=0)}{\boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}'}$ or $\underset{(\text{if } m=1)}{\boldsymbol{u} \hookleftarrow \mathbb{F}^n}$

- PKE.Dec$(\mathsf{ct}, \mathsf{sk} = \boldsymbol{e})$:

  Output $m = \mathsf{ct} \cdot \boldsymbol{e}^T$

Multi-receiver Alekhnovich PKE

- MultiPKE.KeyGen$(1^\lambda, 1^N)$:

  $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_N \hookleftarrow \mathcal{B}er(\sigma)^n$
  $\boldsymbol{G} \hookleftarrow \{\boldsymbol{M} \in \mathbb{F}^{k \times n} \mid \boldsymbol{M}\boldsymbol{e}_i^T = \boldsymbol{0} \text{ forall } i\}$
  Output $\mathsf{pk} = \boldsymbol{G}$ and $(\mathsf{sk}_1, \ldots, \mathsf{sk}_N) = (\boldsymbol{e}_1, \ldots, \boldsymbol{e}_N)$

- MultiPKE.Enc$(m \in \{0,1\}, \mathsf{pk} = \boldsymbol{G}, (\mathsf{sk}_i)_{i \in \mathcal{C}})$:

  $\boldsymbol{e}' \hookleftarrow \mathcal{B}er(\sigma)^n, \boldsymbol{x} \hookleftarrow \mathbb{F}^k, \boldsymbol{y} \hookleftarrow \langle (\mathsf{sk}_i)_{i \in \mathcal{C}} \rangle^\perp$
  Output $\mathsf{ct} = \underset{(\text{if } m = 0)}{\boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}'}$ or $\underset{(\text{if } m = 1)}{\boldsymbol{y} + \boldsymbol{e}'}$

- PKE.Dec$(\mathsf{ct}, \mathsf{sk} = \boldsymbol{e})$:

  Output $m = \mathsf{ct} \cdot \boldsymbol{e}^T$

Inspired from lattice Dual-Regev-based multi-receiver scheme [LPSS14]

[LPSS14]: Ling, Phan, Stehlé, and Steinfeld. Hardness of k-LWE and applications in traitor tracing. (CRYPTO'14)

Decoding Problem with ℓ hints

Distinguish between distributions

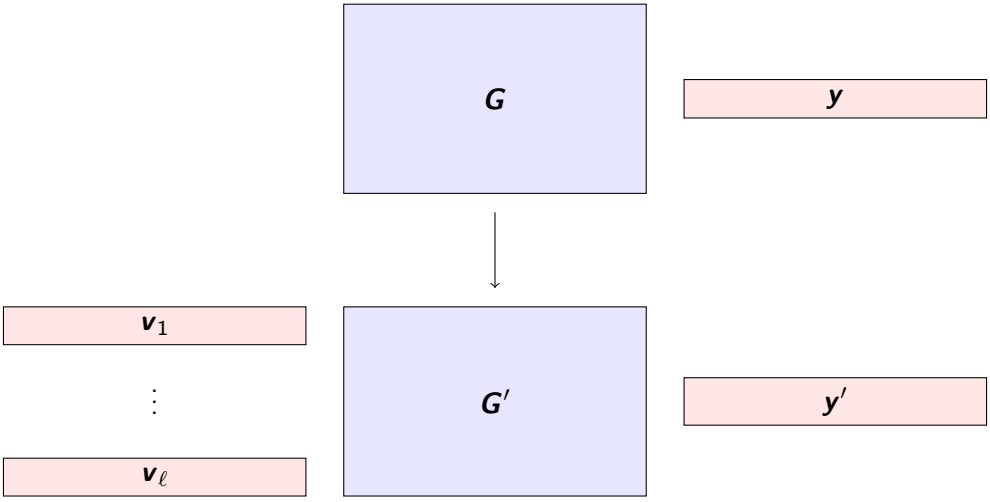
$$(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell, \boldsymbol{G}, \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}) \quad \text{and} \quad (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell, \boldsymbol{G}, \boldsymbol{u} + \boldsymbol{e})$$

for

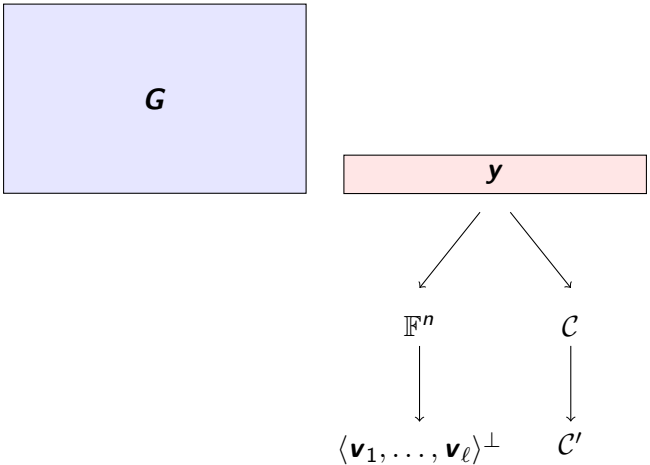
- $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell \hookleftarrow \mathcal{B}er(\sigma)^n, \boldsymbol{G} \hookleftarrow \{\boldsymbol{M} \in \mathbb{F}^{k \times n} \mid \boldsymbol{M}\boldsymbol{v}_i^T = \boldsymbol{0} \text{ forall } i \in [1, \ell]\}$
- $\boldsymbol{e} \hookleftarrow \mathcal{B}er(\omega)^n, \boldsymbol{x} \hookleftarrow \mathbb{F}^k$
- $\boldsymbol{u} \hookleftarrow \langle \boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell \rangle^\perp$

Outline

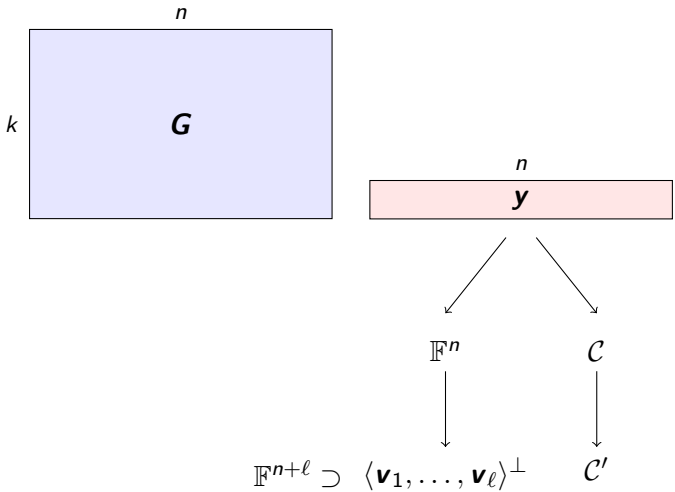
Reduction of security



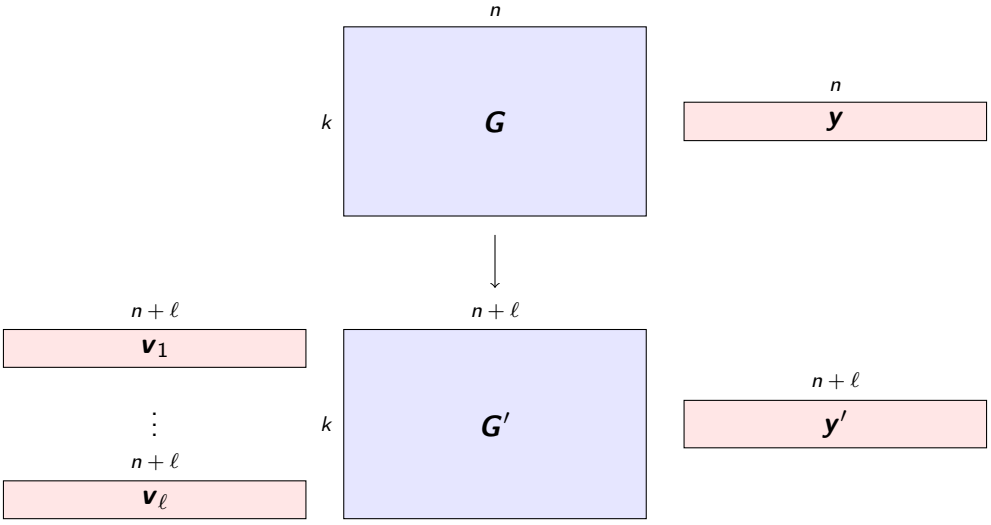
Reduction of security



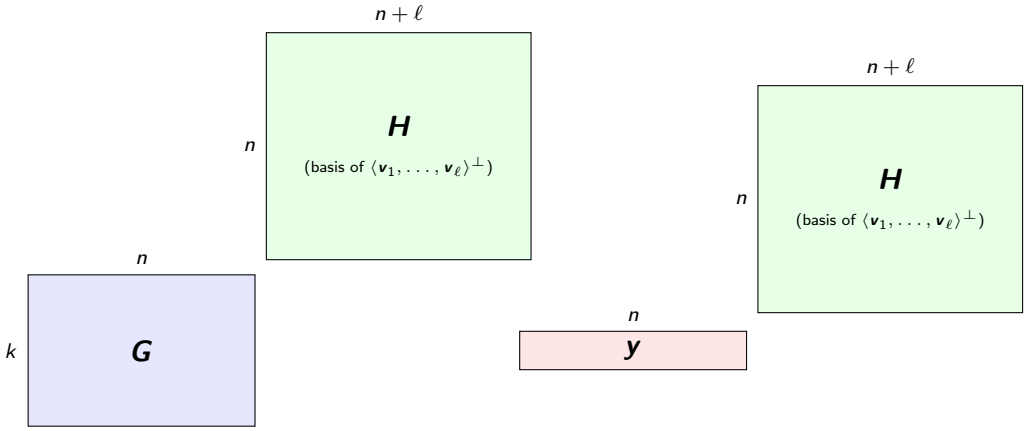
Reduction of security



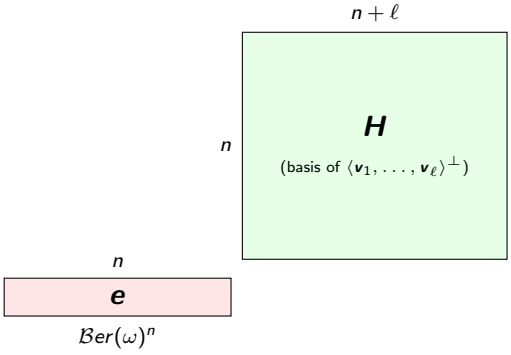
Reduction of security



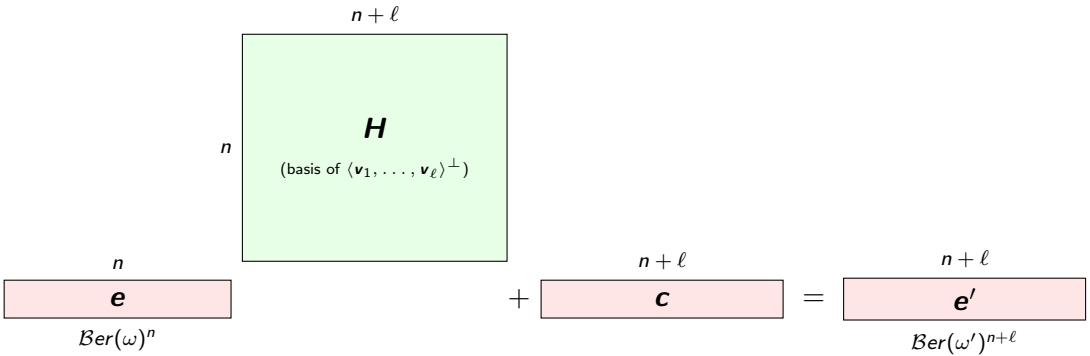
Reduction of security



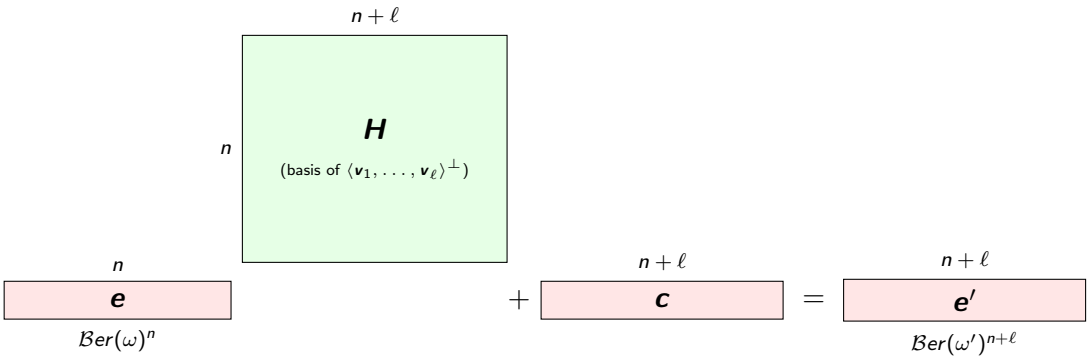
Uncorrelation of skewed Bernoulli noise



Uncorrelation of skewed Bernoulli noise



Uncorrelation of skewed Bernoulli noise



$$\omega' = 2\ell(2\omega)^{\frac{1}{2\ell}}$$

Theorem of the reduction of security

Theorem (Informal)

Consider noise levels ω *and* $\omega' \in \left(2\ell\,(2\omega)^{\frac{1}{2\ell}}, 1/2\right)$. *Then, the generic decoding problem* $\mathrm{DP}(n, k, \omega)$ *reduces to* ℓ-$\mathrm{DP}(n+\ell, k, \omega', \sigma)$.

Reduction is **non tight**; if $\ell \gg 1$, ω' tends quickly to $\frac{1}{2}$

Multi-receiver Alekhnovich PKE

- MultiPKE.KeyGen$(1^\lambda, 1^N)$:

  $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_N \hookleftarrow \mathcal{B}er(\sigma)^n$
  $\boldsymbol{G} \hookleftarrow \{\boldsymbol{M} \in \mathbb{F}^{k \times n} \mid \boldsymbol{M}\boldsymbol{e}_i^T = \boldsymbol{0} \text{ forall } i\}$
  Output $\mathsf{pk} = \boldsymbol{G}$ and $(\mathsf{sk}_1, \ldots, \mathsf{sk}_N) = (\boldsymbol{e}_1, \ldots, \boldsymbol{e}_N)$

- MultiPKE.Enc$(m \in \{0,1\}, \mathsf{pk} = \boldsymbol{G}, (\mathsf{sk}_i)_{i \in \mathcal{C}})$:

  $\boldsymbol{e}' \hookleftarrow \mathcal{B}er(\sigma)^n, \boldsymbol{x} \hookleftarrow \mathbb{F}^k, \boldsymbol{y} \hookleftarrow \langle (\mathsf{sk}_i)_{i \in \mathcal{C}} \rangle^\perp$
  Output $\mathsf{ct} = \underset{(\text{if } m = 0)}{\boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}'}$ or $\underset{(\text{if } m = 1)}{\boldsymbol{y} + \boldsymbol{e}'}$

- PKE.Dec$(\mathsf{ct}, \mathsf{sk} = \boldsymbol{e})$:

  Output $m = \mathsf{ct} \cdot \boldsymbol{e}^T$

Perspectives: compact multi-receiver Alekhnovich PKE with MDPC codes

- MultiPKE.KeyGen$(1^\lambda, 1^N)$:

  $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_N \hookleftarrow \mathcal{C}^{\perp}_{\text{MDPC}}$
  $\boldsymbol{G} \hookleftarrow \{\boldsymbol{M} \in \mathbb{F}^{k \times n} \mid \boldsymbol{M}\boldsymbol{e}_i^T = \boldsymbol{0} \text{ forall } i\}$
  Output $\text{pk} = \boldsymbol{G}$ and $(\text{sk}_1, \ldots, \text{sk}_N) = (\boldsymbol{e}_1, \ldots, \boldsymbol{e}_N)$

- MultiPKE.Enc$(m \in \{0,1\}, \text{pk} = \boldsymbol{G}, (\text{sk}_i)_{i \in \mathcal{C}})$:

  $\boldsymbol{e}' \hookleftarrow \mathcal{B}er(\sigma)^n, \boldsymbol{x} \hookleftarrow \mathbb{F}^k, \boldsymbol{y} \hookleftarrow \langle (\text{sk}_i)_{i \in \mathcal{C}} \rangle^{\perp}$
  Output $\text{ct} = \underset{(\text{if } m = 0)}{\boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}'}$ or $\underset{(\text{if } m = 1)}{\boldsymbol{y} + \boldsymbol{e}'}$

- PKE.Dec$(\text{ct}, \text{sk} = \boldsymbol{e})$:

  Output $m = \text{ct} \cdot \boldsymbol{e}^T$

MDPC-Decoding Problem with ℓ hints

Distinguish between distributions

$$(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell, \boldsymbol{G}, \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}) \quad \text{and} \quad (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell, \boldsymbol{G}, \boldsymbol{u} + \boldsymbol{e})$$

for

- $\boldsymbol{G} \hookleftarrow$ MDPC matrix, $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell \hookleftarrow \mathcal{C}_{\boldsymbol{G}}^{\perp}$ of short Hamming weight
- $\boldsymbol{e} \hookleftarrow \mathcal{B}er(\omega)^n, \boldsymbol{x} \hookleftarrow \mathbb{F}^k$
- $\boldsymbol{u} \hookleftarrow \langle \boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell \rangle^{\perp}$

MDPC-Decoding Problem with ℓ hints

Distinguish between distributions

$$(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell, \boldsymbol{G}, \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}) \quad \text{and} \quad (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell, \boldsymbol{G}, \boldsymbol{u} + \boldsymbol{e})$$

for

- $\boldsymbol{G} \hookleftarrow$ MDPC matrix, $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell \hookleftarrow \mathcal{C}_{\boldsymbol{G}}^{\perp}$ of short Hamming weight
- $\boldsymbol{e} \hookleftarrow \mathcal{B}er(\omega)^n, \boldsymbol{x} \hookleftarrow \mathbb{F}^k$
- $\boldsymbol{u} \hookleftarrow \langle \boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell \rangle^{\perp}$

Thanks for your attention!

`https://eprint.iacr.org/2025/2151`

References I


San Ling, Duong Hieu Phan, Damien Stehlé, and Ron Steinfeld.
Hardness of k-LWE and applications in traitor tracing.
In Juan A. Garay and Rosario Gennaro, editors, CRYPTO 2014, Part I, volume 8616 of LNCS, pages 315–334. Springer, Heidelberg, August 2014.

IND-CPA security game with revocation

Adversary		**Challenger**
Chooses $\mathcal{C}$		$(\mathsf{pk}, (\mathsf{sk}_1, \ldots, \mathsf{sk}_N)) \leftarrow \mathsf{MultiPKE.KeyGen}(1^\lambda, 1^N)$
	$\mathcal{C} \longrightarrow$	
	$\longleftarrow \mathsf{pk}, (\mathsf{sk}_i)_{i \in \mathcal{C}}$	
Chooses m_0, m_1	$m_0, m_1 \longrightarrow$	
		Checks $\lvert m_0 \rvert = \lvert m_1 \rvert$
		$b \leftarrow\$ \{0, 1\}$
	$\longleftarrow \mathsf{MultiPKE.Enc}(m_b, \mathsf{pk}, (\mathsf{sk}_i)_{i \in \mathcal{C}})$	
Chooses b^*		

Adversary wins if $b = b^*$