The Kernel Matrix Diffie-Hellman Assumption

Carla Ràfols[1], Paz Morillo[2] and Jorge L. Villar[2]

[1] Universitat Pompeu Fabra (UPF) Spain

[2] Universitat Politècnica de Catalunya (UPC) Spain

MAK

Matemática Aplicada a la Criptografía

Asiacrypt 2016, Hanoi, 8 Dec 2016

Outline

Additive (Implicit) Notation

Given a group $\mathcal{G}$ of prime order q and a generator $g \in \mathcal{G}$:

$$
\begin{array}{lcl}
g^x & \rightarrow & [x] \\
g & \rightarrow & [1] \\
1 & \rightarrow & [0] \\
g^x g^y & \rightarrow & [x][y] = [x+y] \\
(g^x)^y & \rightarrow & [x]^y = [xy] \\
(g^{x_1}, \ldots, g^{x_n}) & \rightarrow & [x_1, \ldots, x_n] \\
\begin{pmatrix} g^{x_{11}} & \cdots & g^{x_{1m}} \\ \vdots & & \vdots \\ g^{x_{n1}} & \cdots & g^{x_{nm}} \end{pmatrix} & \rightarrow & \begin{bmatrix} x_{11} & \cdots & x_{1m} \\ \vdots & & \vdots \\ x_{n1} & \cdots & x_{nm} \end{bmatrix}
\end{array}
$$

Given a (symmetric) bilinear map $e : \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}_T$:

$$e(g^x, g^y) = g_T^{xy} \quad \rightarrow \quad e([x],[y]) = [xy]_T$$

Subspace Membership Problems

For a (k, ℓ)-collection of vector subspaces of dimension k, $\mathcal{S} = \{S_i\}_{i \in \mathcal{I}}$, of the vector space $\mathbb{Z}_q^\ell$, where $0 < k < \ell$

Definition (Subspace Membership Problem)

Given $\mathcal{G}$ and g, tell apart

$D_{\text{real}} = ([S], [\boldsymbol{z}])$ for random $S \leftarrow \mathcal{S}$ and $\boldsymbol{z} \leftarrow S$

$D_{\text{random}} = ([S], [\boldsymbol{z}])$ for random $S \leftarrow \mathcal{S}$ and $\boldsymbol{z} \leftarrow \mathbb{Z}_q^\ell$

Subspace Membership Problems

For a (k, ℓ)-collection of vector subspaces of dimension k, $\mathcal{S} = \{S_i\}_{i \in \mathcal{I}}$, of the vector space $\mathbb{Z}_q^\ell$, where $0 < k < \ell$

Definition (Subspace Membership Problem)

Given $\mathcal{G}$ and g, tell apart

$D_{\text{real}} = ([S], [\boldsymbol{z}])$ for random $S \leftarrow \mathcal{S}$ and $\boldsymbol{z} \leftarrow S$

$D_{\text{random}} = ([S], [\boldsymbol{z}])$ for random $S \leftarrow \mathcal{S}$ and $\boldsymbol{z} \leftarrow \mathbb{Z}_q^\ell$

Typically, $S = \operatorname{Span} A$, where $A \in \mathbb{Z}_q^{\ell \times k}$ and $\operatorname{rank} A = k$.

Subspace Membership Problems

DDH: $A(a) = \begin{pmatrix} 1 \\ a \end{pmatrix}$ $\quad a \leftarrow \mathbb{Z}_q$

$$\boldsymbol{z} = \begin{pmatrix} 1 \\ a \end{pmatrix} (w) = \begin{pmatrix} w \\ aw \end{pmatrix} \text{ vs. } \boldsymbol{z} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$$

2-Lin: $A(a_1, a_2) = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \\ 1 & 1 \end{pmatrix}$ $\quad a_1, a_2 \leftarrow \mathbb{Z}_q$

$$\boldsymbol{z} = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} a_1 w_1 \\ a_2 w_2 \\ w_1 + w_2 \end{pmatrix} \text{ vs. } \boldsymbol{z} = \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix}$$

Subspace Membership Problems

DDH: $A(a) = \begin{pmatrix} 1 \\ a \end{pmatrix}$ $\quad a \leftarrow \mathbb{Z}_q$

$\boldsymbol{z} = \begin{pmatrix} 1 \\ a \end{pmatrix}(w) = \begin{pmatrix} w \\ aw \end{pmatrix}$ vs. $\boldsymbol{z} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$

"Matrix distributions"

2-Lin: $A(a_1, a_2) = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \\ 1 & 1 \end{pmatrix}$ $\quad a_1, a_2 \leftarrow \mathbb{Z}_q$

$\boldsymbol{z} = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} a_1 w_1 \\ a_2 w_2 \\ w_1 + w_2 \end{pmatrix}$ vs. $\boldsymbol{z} = \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix}$

Matrix Distributions

Given $1 \leq k < \ell$,

Definition (Polynomial Matrix Distribution)

$A \leftarrow \mathcal{D}^f_{\ell,k}$, where $A \in \mathbb{Z}_q^{\ell \times k}$, $\operatorname{rank} A = k$ and A is sampled according to $A = f(a_1, \ldots, a_d)$, where $a_1, \ldots, a_d \leftarrow \mathbb{Z}_q$ and f is a polynomial map of constant degree.

Matrix Distributions

Given $1 \leq k < \ell$,

Definition (Polynomial Matrix Distribution)

$A \leftarrow \mathcal{D}^f_{\ell,k}$, where $A \in \mathbb{Z}_q^{\ell \times k}$, $\operatorname{rank} A = k$ and A is sampled according to $A = f(a_1, \ldots, a_d)$, where $a_1, \ldots, a_d \leftarrow \mathbb{Z}_q$ and f is a polynomial map of constant degree.

- We also tolerate $\Pr(\operatorname{rank} A < k) \in$ **negl**.
- We focus on the case $\ell = k + 1$, and $\deg f = 1$

Matrix Distributions

Given $1 \leq k < \ell$,

Definition (Polynomial Matrix Distribution)

$A \leftarrow \mathcal{D}^f_{\ell,k}$, where $A \in \mathbb{Z}_q^{\ell \times k}$, $\operatorname{rank} A = k$ and A is sampled according to $A = f(a_1, \ldots, a_d)$, where $a_1, \ldots, a_d \leftarrow \mathbb{Z}_q$ and f is a polynomial map of constant degree.

- We also tolerate $\Pr(\operatorname{rank} A < k) \in \mathbf{negl}$.
- We focus on the case $\ell = k + 1$, and $\deg f = 1$

E.g. $\quad A(a) = \begin{pmatrix} 1 \\ a \end{pmatrix} \qquad A(a_1, a_2) = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \\ 1 & 1 \end{pmatrix}$

Matrix Decision Diffie-Hellman (MDDH) Problems

Definition ($\mathcal{D}^A_{\ell,k}$-MDDH Problem [EHKRV13])

Tell apart the two probability distributions

$$D_{\text{real}} = (\mathcal{G}, q, g, [A(\boldsymbol{t})], [A(\boldsymbol{t})\boldsymbol{w}]), \;\; \boldsymbol{t} \leftarrow \mathbb{Z}_q^d, \;\; \boldsymbol{w} \leftarrow \mathbb{Z}_q^k$$

$$D_{\text{random}} = (\mathcal{G}, q, g, [A(\boldsymbol{t})], [\boldsymbol{z}]), \;\; \boldsymbol{t} \leftarrow \mathbb{Z}_q^d, \;\; \boldsymbol{z} \leftarrow \mathbb{Z}_q^\ell$$

The $\mathcal{D}^A_{\ell,k}$-MDDH Assumption states that the above problem is hard, w.r.t. and instance generator $(q, \mathcal{G}, g) \leftarrow \mathcal{I}$

Matrix Decision Diffie-Hellman (MDDH) Problems

Definition ($\mathcal{D}^A_{\ell,k}$-MDDH Problem [EHKRV13])

Tell apart the two probability distributions

$$D_{\text{real}} = (\mathcal{G}, q, g, [A(\boldsymbol{t})], [A(\boldsymbol{t})\boldsymbol{w}]), \;\; \boldsymbol{t} \leftarrow \mathbb{Z}_q^d, \;\; \boldsymbol{w} \leftarrow \mathbb{Z}_q^k$$

$$D_{\text{random}} = (\mathcal{G}, q, g, [A(\boldsymbol{t})], [\boldsymbol{z}]), \;\; \boldsymbol{t} \leftarrow \mathbb{Z}_q^d, \;\; \boldsymbol{z} \leftarrow \mathbb{Z}_q^\ell$$

The $\mathcal{D}^A_{\ell,k}$-MDDH Assumption states that the above problem is hard, w.r.t. and instance generator $(q, \mathcal{G}, g) \leftarrow \mathcal{I}$

Generic hardness depends on the degree and irreducibility of the **determinant polynomial** $\mathfrak{d}(\boldsymbol{t}, \boldsymbol{z}) = \det(A(\boldsymbol{t}) \| \boldsymbol{z})$

Known Instances

$$A_{k\text{-Unif}} = \begin{pmatrix} t_{1,1} & \cdots & t_{1,k} \\ \vdots & \ddots & \vdots \\ t_{k+1,1} & \cdots & t_{k+1,k} \end{pmatrix} \qquad A_{k\text{-Lin}} = \begin{pmatrix} t_1 & 0 & \cdots & 0 \\ 0 & t_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & t_k \\ 1 & 1 & \cdots & 1 \end{pmatrix}$$

$$A_{k\text{-Casc}} = \begin{pmatrix} t_1 & 0 & \cdots & 0 \\ 1 & t_2 & \ddots & \vdots \\ 0 & \ddots & \ddots & 0 \\ \vdots & \ddots & 1 & t_k \\ 0 & \cdots & 0 & 1 \end{pmatrix} \qquad A_{k\text{-SCasc}} = \begin{pmatrix} t & 0 & \cdots & 0 \\ 1 & t & \ddots & \vdots \\ 0 & \ddots & \ddots & 0 \\ \vdots & \ddots & 1 & t \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Applications

Some known applications:

- Public key encryption
- Hash Proof systems
- Pseudorandom functions
- Non-interactive Zero-Knowledge proofs (Groth-Sahai)
- Efficient Proofs for CRS-Dependent Languages

Key idea: Most constructions based on DDH or 2-Lin are actually valid for any MDDH problem

We can obtain

- more compact instances
- more secure instances (secure even when an efficient multilinear map is available)

Outline

Flexible Computational Matrix Problems

Decision problems: natural model for indistinguishability adversarial capabilities (IND-CPA, pseudorandomness,...).

Flexible Computational Matrix Problems

Decision problems: natural model for indistinguishability adversarial capabilities (IND-CPA, pseudorandomness,...).

(Flexible) computational problems: Capture forgery adversarial capabilities. E.g. breaking

- unforgeability of a digital signature
- soundness of a ZK argument
- binding property of a commitment
- ...

Flexible Computational Matrix Problems

Decision problems: natural model for indistinguishability adversarial capabilities (IND-CPA, pseudorandomness,...).

(Flexible) computational problems: Capture forgery adversarial capabilities. E.g. breaking

- unforgeability of a digital signature
- soundness of a ZK argument
- binding property of a commitment
- ...

We unify some existing flexible computational problems in the literature in a single framework.

The Kernel Matrix Diffie-Hellman Assumption

For a (r, ℓ)-collection of vector subspaces of dimension r, $\mathcal{S} = \{S_i\}_{i \in \mathcal{I}}$, of the vector space $\mathbb{Z}_q^\ell$, where $0 < r < \ell$

Definition (Subspace Sampling Problem)

Given $\mathcal{G}$, g and $[S]$, find $[\boldsymbol{x}]$ where $\boldsymbol{x}$ is a nonzero vector in S

Typically $S = \ker A^\top$, where $A \in \mathbb{Z}_q^{\ell \times k}$, $\operatorname{rank} A = k$ and $r = \ell - k$.

The Kernel Matrix Diffie-Hellman Assumption

For a (r, ℓ)-collection of vector subspaces of dimension r, $\mathcal{S} = \{S_i\}_{i \in \mathcal{I}}$, of the vector space $\mathbb{Z}_q^\ell$, where $0 < r < \ell$

Definition (Subspace Sampling Problem)

Given $\mathcal{G}$, g and $[S]$, find $[\boldsymbol{x}]$ where $\boldsymbol{x}$ is a nonzero vector in S

Typically $S = \ker A^\top$, where $A \in \mathbb{Z}_q^{\ell \times k}$, $\operatorname{rank} A = k$ and $r = \ell - k$.

Definition ($\mathcal{D}_{\ell,k}^A$-KerMDH Problem)

Given $[A]$, where $A \leftarrow \mathcal{D}_{\ell,k}$ find a nonzero vector $[\boldsymbol{x}]$ such that $\boldsymbol{x}^\top A = \mathbf{0}$.

The $\mathcal{D}_{\ell,k}^A$-KerDH Assumption states that the above problem is hard, w.r.t. and instance generator $(q, \mathcal{G}, g) \leftarrow \mathcal{I}$

KerMDH Examples

DDH Kernel: $A(a) = \begin{pmatrix} 1 \\ a \end{pmatrix} \quad a \leftarrow \mathbb{Z}_q$

Given $[A]$, find $[x_1, x_2] \neq [\mathbf{0}]$ such that

$$\begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} 1 \\ a \end{pmatrix} = x_1 + a x_2 = 0$$

2-Lin Kernel: $A(a_1, a_2) = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \\ 1 & 1 \end{pmatrix} \quad a_1, a_2 \leftarrow \mathbb{Z}_q$

Given $[A]$, find $[x_1, x_2, x_3] \neq [\mathbf{0}]$ such that

$$\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} a_1 x_1 + x_3 & a_2 x_2 + x_3 \end{pmatrix} = \mathbf{0}$$

KerMDH Examples

DDH Kernel: $A(a) = \begin{pmatrix} 1 \\ a \end{pmatrix} \quad a \leftarrow \mathbb{Z}_q$

Given $[A]$, find $[x_1, x_2] \neq [\mathbf{0}]$ such that

$$\begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} 1 \\ a \end{pmatrix} = x_1 + a x_2 = 0$$

Just Take
$[x_1, x_2] = [-a, 1]$!

2-Lin Kernel: $A(a_1, a_2) = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \\ 1 & 1 \end{pmatrix} \quad a_1, a_2 \leftarrow \mathbb{Z}_q$

Given $[A]$, find $[x_1, x_2, x_3] \neq [\mathbf{0}]$ such that

$$\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} a_1 x_1 + x_3 & a_2 x_2 + x_3 \end{pmatrix} = \mathbf{0}$$

KerMDH Examples

DDH Kernel: $A(a) = \begin{pmatrix} 1 \\ a \end{pmatrix} \quad a \leftarrow \mathbb{Z}_q$

Given $[A]$, find $[x_1, x_2] \neq [\mathbf{0}]$ such that

$$\begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} 1 \\ a \end{pmatrix} = x_1 + a x_2 = 0$$

Just Take
$[x_1, x_2] = [-a, 1]$!

2-Lin Kernel: $A(a_1, a_2) = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \\ 1 & 1 \end{pmatrix} \quad a_1, a_2 \leftarrow \mathbb{Z}_q$

Given $[A]$, find $[x_1, x_2, x_3] \neq [\mathbf{0}]$ such that

$$\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} a_1 x_1 + x_3 & a_2 x_2 + x_3 \end{pmatrix} = \mathbf{0}$$

$[x_1, x_2, x_3] = [-a_2\lambda, -a_1\lambda, a_1 a_2 \lambda]$ for some λ.
Hard to compute from $[a_1]$, $[a_2]$!

More Examples

Lemma (KerMDH vs. MDDH)

In pairing groups, $\mathcal{D}^A_{\ell,k}$-MDDH $\Rightarrow$ $\mathcal{D}^A_{\ell,k}$-KerDH

D_{real}:

$$\boldsymbol{x}^\top A\boldsymbol{w} = 0 \quad \Rightarrow \quad \boldsymbol{x}^\top(A\boldsymbol{w}) = 0 \quad \Rightarrow \quad e([\boldsymbol{x}^\top], [A\boldsymbol{w}]) = [0]_T$$

D_{random}:

$$\boldsymbol{z} \leftarrow \mathbb{Z}_q^\ell \quad \Rightarrow \quad \boldsymbol{x}^\top\boldsymbol{z} \neq 0 \quad \Rightarrow \quad e([\boldsymbol{x}^\top], [A\boldsymbol{w}]) \neq [0]_T \quad \text{w.o.p.}$$

More Examples

Lemma (KerMDH vs. MDDH)

In pairing groups, $\mathcal{D}^A_{\ell,k}$-MDDH $\Rightarrow$ $\mathcal{D}^A_{\ell,k}$-KerDH

D_{real}:

$$\boldsymbol{x}^\top A\boldsymbol{w} = 0 \quad \Rightarrow \quad \boldsymbol{x}^\top(A\boldsymbol{w}) = 0 \quad \Rightarrow \quad e([\boldsymbol{x}^\top], [A\boldsymbol{w}]) = [0]_T$$

D_{random}:

$$\boldsymbol{z} \leftarrow \mathbb{Z}_q^\ell \quad \Rightarrow \quad \boldsymbol{x}^\top\boldsymbol{z} \neq 0 \quad \Rightarrow \quad e([\boldsymbol{x}^\top], [A\boldsymbol{w}]) \neq [0]_T \quad \text{w.o.p.}$$

All hard MDDH instances define hard KerMDH instances:
k-Unif, k-Lin, k-Casc, k-SCasc, ...

The KerMDH Family

- KerMDH integrates some previously known assumptions:
  - Find-Rep [Brands93]
  - Simultaneous Double Pairing [AFGHO10]
  - Triple Pairing [Groth10]
  - Simultaneous Pairing [GL07]
  - 1-Flexible Diffie-Hellman [LV08]
  - 1-Flexible Square Diffie-Hellman [LPV05]

The KerMDH Family

- KerMDH integrates some previously known assumptions:
  - Find-Rep [Brands93]
  - Simultaneous Double Pairing [AFGHO10]
  - Triple Pairing [Groth10]
  - Simultaneous Pairing [GL07]
  - 1-Flexible Diffie-Hellman [LV08]
  - 1-Flexible Square Diffie-Hellman [LPV05]
- Applications:
  - Homomorphic Signatures [LPJY13]
  - Quasi-Adaptive NIZK [KW15]
  - Trapdoor Commitments to Group Elements
  - Structure Preserving Signatures [KPW15], . . .

The power of KerMDH

Designated-verifier proof of membership:

Given $[\boldsymbol{x}]$ and $[M]$, prove that $\boldsymbol{x} = M\boldsymbol{w}$ for some $\boldsymbol{w}$.

Designated verifier keys: Secret K, public $[M^\top K]$.

Proof: $[\pi]$ such that $\pi^\top = \boldsymbol{x}^\top K$.

($[\pi^\top] = [\boldsymbol{w}^\top M^\top K]$ fulfils the equation)

The power of KerMDH

Designated-verifier proof of membership:

Given $[\boldsymbol{x}]$ and $[M]$, prove that $\boldsymbol{x} = M\boldsymbol{w}$ for some $\boldsymbol{w}$.

Designated verifier keys: Secret K, public $[M^\top K]$.

Proof: $[\pi]$ such that $\pi^\top = \boldsymbol{x}^\top K$.

($[\pi^\top] = [\boldsymbol{w}^\top M^\top K]$ fulfils the equation)

Using $\mathcal{D}_{\ell,k}$-KerDH, Publicly verifiable proof:

Public parameters: $[M], [M^\top K], [A], [KA]$, $A \leftarrow \mathcal{D}_{\ell,k}$.

Proof: $[\pi]$ such that $e([\pi^\top], [A]) = e([\boldsymbol{x}^\top], [KA])$.

$$\pi^\top A = \boldsymbol{x}^\top KA \quad \Leftrightarrow \quad (\pi^\top - \boldsymbol{x}^\top K)A = \mathbf{0} \quad \Rightarrow \quad \pi^\top = \boldsymbol{x}^\top K$$

or $\mathcal{D}_{\ell,k}$-KerDH is easy.

Outline

Hardness of KerDH

- **Hard instances:** $\mathcal{D}_{\ell,k}$ hard for $k > 1$, implies that $\mathcal{D}_{\ell,k}$-*KerDH* is hard in the generic k-linear group model

Hardness of KerDH

- **Hard instances:** $\mathcal{D}_{\ell,k}$ hard for $k > 1$, implies that $\mathcal{D}_{\ell,k}$-*KerDH* is hard in the generic k-linear group model
- **Algebraic Reductions:**
  If $B = LAR$ then $\mathcal{D}^B_{\ell,k}$-*KerDH* $\Rightarrow$ $\mathcal{D}^A_{\ell,k}$-*KerDH*

Hardness of KerDH

- **Hard instances:** $\mathcal{D}_{\ell,k}$ hard for $k > 1$, implies that $\mathcal{D}_{\ell,k}$-*KerDH* is hard in the generic k-linear group model
- **Algebraic Reductions:**
  If $B = LAR$ then $\mathcal{D}^B_{\ell,k}$-*KerDH* $\Rightarrow$ $\mathcal{D}^A_{\ell,k}$-*KerDH*
- **Increasing Hardness:** For the typical families of hard $\mathcal{D}_{\ell,k}$ of increasing size
  $\mathcal{D}^A_{k+1}$-*KerDH* $\Rightarrow$ $\mathcal{D}^A_k$-*KerDH*

  $\mathcal{D}^A_{k+1}$-*KerDH* $\not\Rightarrow$ $\mathcal{D}^A_k$-*KerDH*

Hardness of KerDH

- **Hard instances:** $\mathcal{D}_{\ell,k}$ hard for $k > 1$, implies that $\mathcal{D}_{\ell,k}$-*KerDH* is hard in the generic k-linear group model
- **Algebraic Reductions:** If $B = LAR$ then $\mathcal{D}^B_{\ell,k}$-*KerDH* $\Rightarrow$ $\mathcal{D}^A_{\ell,k}$-*KerDH*
- **Increasing Hardness:** For the typical families of hard $\mathcal{D}_{\ell,k}$ of increasing size $\mathcal{D}^A_{k+1}$-*KerDH* $\Rightarrow$ $\mathcal{D}^A_k$-*KerDH*

$\mathcal{D}^A_{k+1}$-*KerDH* $\not\Leftarrow$ $\mathcal{D}^A_k$-*KerDH* **Explicit Reductions**

Hardness of KerDH

- **Hard instances:** $\mathcal{D}_{\ell,k}$ hard for $k > 1$, implies that $\mathcal{D}_{\ell,k}$-*KerDH* is hard in the generic k-linear group model
- **Algebraic Reductions:** If $B = LAR$ then $\mathcal{D}^B_{\ell,k}$-*KerDH* $\Rightarrow$ $\mathcal{D}^A_{\ell,k}$-*KerDH*
- **Increasing Hardness:** For the typical families of hard $\mathcal{D}_{\ell,k}$ of increasing size $\mathcal{D}^A_{k+1}$-*KerDH* $\Rightarrow$ $\mathcal{D}^A_k$-*KerDH*

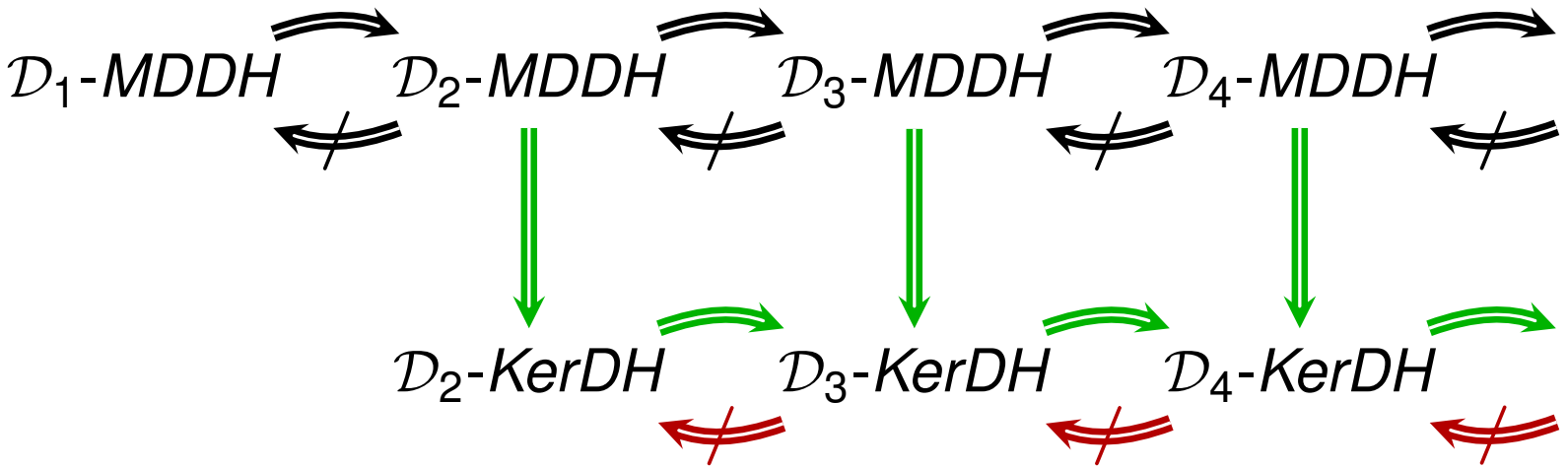
$\mathcal{D}^A_{k+1}$-*KerDH* $\not\Rightarrow$ $\mathcal{D}^A_k$-*KerDH*

Black-Box Separation

Explicit Reductions

Families with Increasing Hardness

[EHKRV13]



[This work]

Valid for all families: k-Unif, k-Lin, k-Casc, k-SCasc.

Black-Box Separations

$\mathcal{P}_1 \overset{\text{BB}}{\Rightarrow} \mathcal{P}_2$ means that a reduction $\mathcal{R}$ solves $\mathcal{P}_1$ using **any** possible oracle solving $\mathcal{P}_2$.

Black-Box Separations

$\mathcal{P}_1 \overset{\text{BB}}{\Rightarrow} \mathcal{P}_2$ means that a reduction $\mathcal{R}$ solves $\mathcal{P}_1$ using **any** possible oracle solving $\mathcal{P}_2$.

Black-box reductions between flexible problems are hard to find (or they are very natural)

($\mathcal{R}$ must work for **all** possible solutions of $\mathcal{P}_2$.)

Black-Box Separations

$\mathcal{P}_1 \overset{\text{BB}}{\Rightarrow} \mathcal{P}_2$ means that a reduction $\mathcal{R}$ solves $\mathcal{P}_1$ using **any** possible oracle solving $\mathcal{P}_2$.

Black-box reductions between flexible problems are hard to find (or they are very natural)

($\mathcal{R}$ must work for **all** possible solutions of $\mathcal{P}_2$.)

Black-box separation means that every BB reduction fails for some oracle for $\mathcal{P}_2$.

Black-Box Separations

$\mathcal{P}_1 \overset{\text{BB}}{\Rightarrow} \mathcal{P}_2$ means that a reduction $\mathcal{R}$ solves $\mathcal{P}_1$ using **any** possible oracle solving $\mathcal{P}_2$.

Black-box reductions between flexible problems are hard to find (or they are very natural)

($\mathcal{R}$ must work for **all** possible solutions of $\mathcal{P}_2$.)

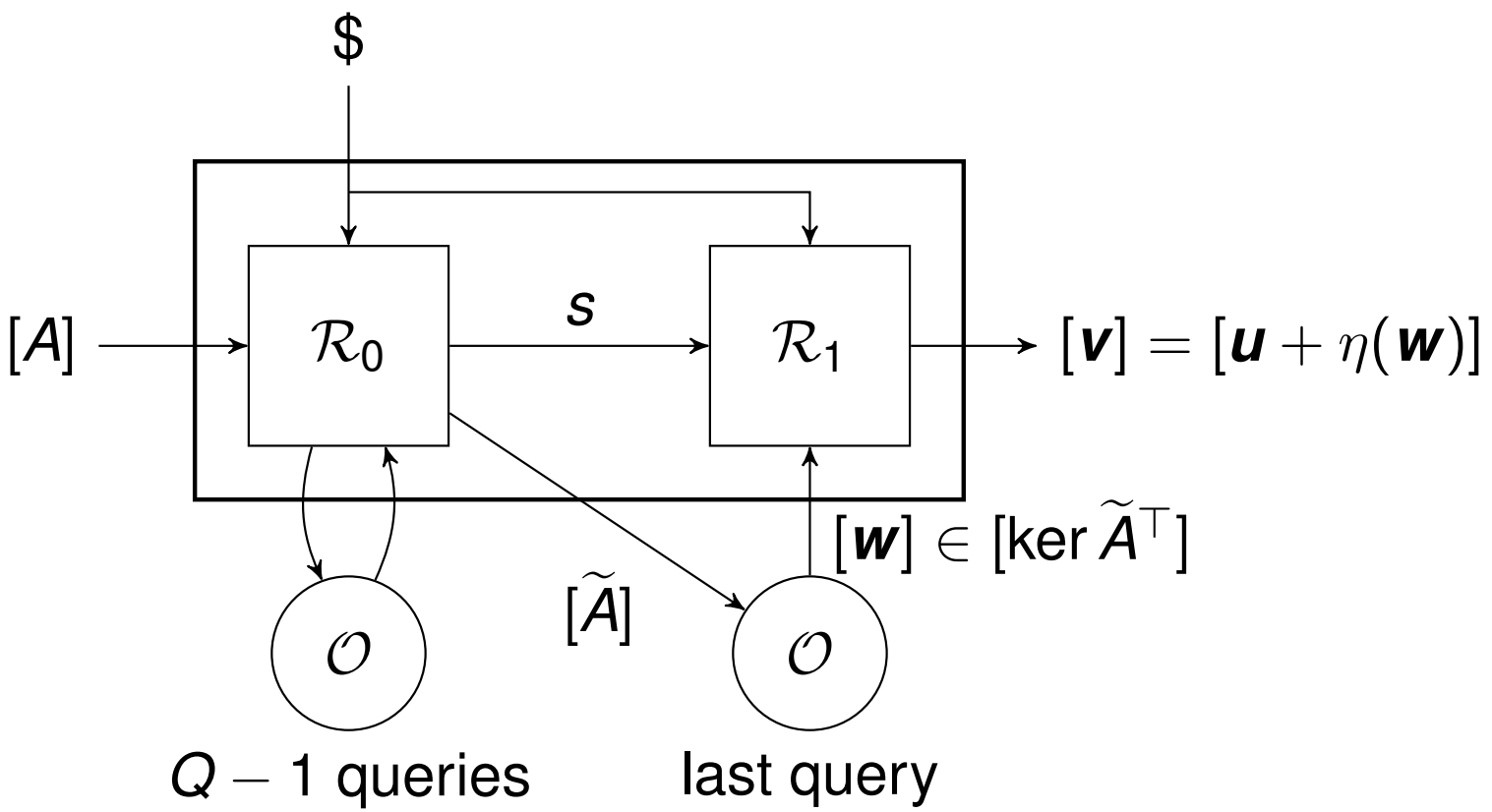
Black-box separation means that every BB reduction fails for some oracle for $\mathcal{P}_2$.

We impose some extra requirements to $\mathcal{R}$:

- It is generic (it works on the generic k-linear group model),
- It makes a constant number of calls Q to the $\mathcal{P}_2$ oracle.

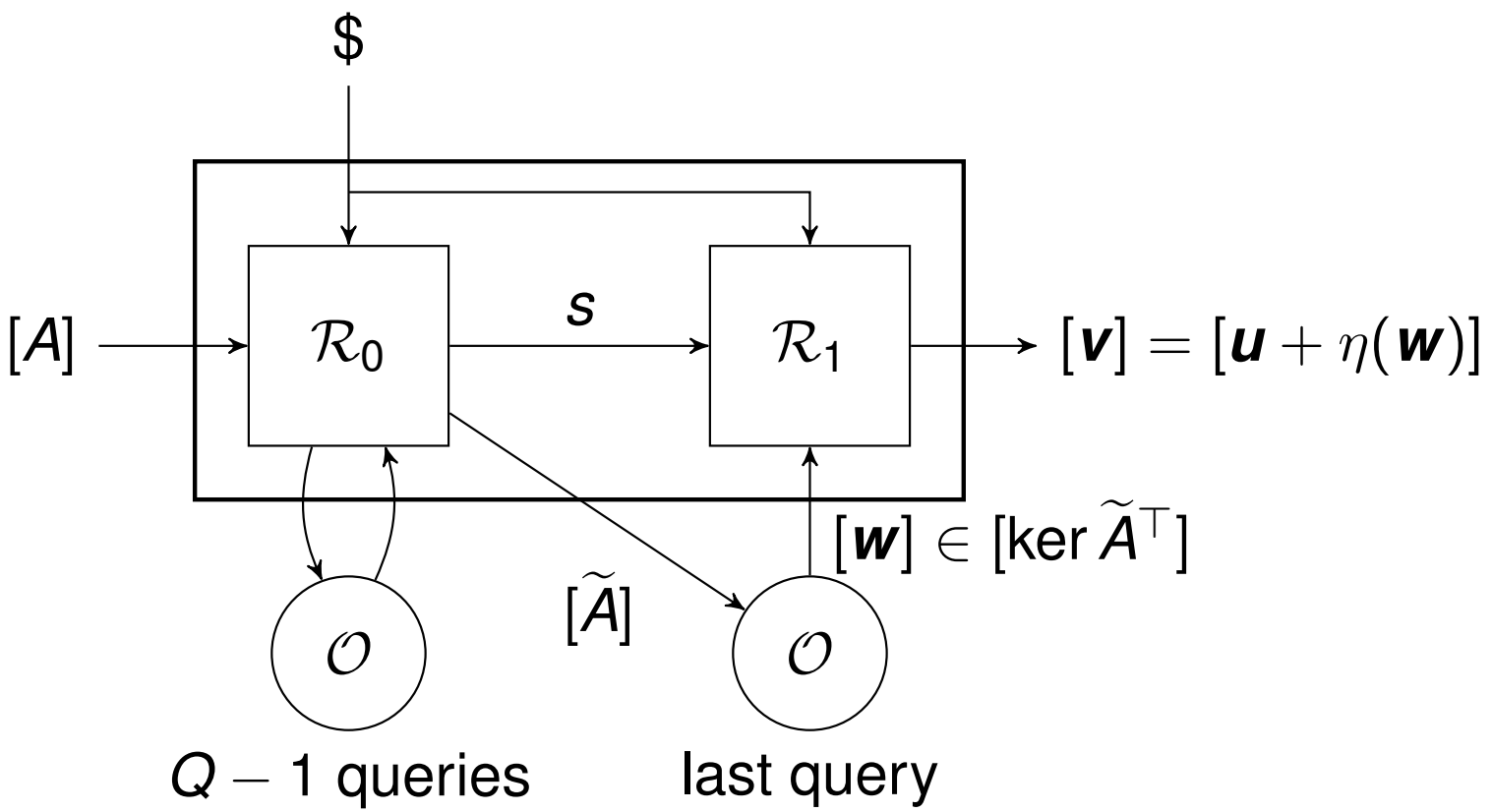
BB Separation: Reduction Splitting

$$\mathcal{D}_{\ell,k}\text{-KerDH} \overset{\mathcal{R}}{\Rightarrow} \mathcal{D}_{\widetilde{\ell},\widetilde{k}}\text{-KerDH for } k > \widetilde{k}$$



BB Separation: Reduction Splitting

$$\mathcal{D}_{\ell,k}\text{-KerDH} \overset{\mathcal{R}}{\Rightarrow} \mathcal{D}_{\widetilde{\ell},\widetilde{k}}\text{-KerDH for } k > \widetilde{k}$$



- Generic model: η is linear and it only depends on \$.
- dim $Im(\eta) < k$

BB Separation: Query Supression

Definition (k-Elusiveness)

A (r, ℓ)-collection of vector subspaces $\mathcal{S}$ is k-elusive if given any k-vector subspace F,

$$\Pr[S \cap F \neq \{\mathbf{0}\} : S \leftarrow \mathcal{S}] \in \mathbf{negl}$$

BB Separation: Query Supression

Definition (k-Elusiveness)

A (r, ℓ)-collection of vector subspaces $\mathcal{S}$ is k-elusive if given any k-vector subspace F,

$$\Pr[S \cap F \neq \{\mathbf{0}\} : S \leftarrow \mathcal{S}] \in \mathbf{negl}$$

Lemma

For any hard matrix distribution $\mathcal{D}_{\ell,k}$, the collection of subspaces $\{\ker A^\top\}_{A \in \mathcal{D}_{\ell,k}}$ is k-elusive.

BB Separation: Query Supression

Definition (k-Elusiveness)

A (r, ℓ)-collection of vector subspaces $\mathcal{S}$ is k-elusive if given any k-vector subspace F,

$$\Pr[S \cap F \neq \{\mathbf{0}\} : S \leftarrow \mathcal{S}] \in \mathbf{negl}$$

Lemma

For any hard matrix distribution $\mathcal{D}_{\ell,k}$, the collection of subspaces $\{\ker A^\top\}_{A \in \mathcal{D}_{\ell,k}}$ is k-elusive.

We prove the last oracle call does not help the reduction.

By induction, if $\mathcal{R}$ exists then $\mathcal{D}_{\ell,k}$-KerDH can be solved directly (e.g. $Q = 0$).

Larger Kernel Problems are strictly harder!

Outline

A New Matrix Distribution With $\ell > k+1$

(k,d)-Circ: A compact hard matrix distribution with $\ell > k+1$

$$A_{(k,d)\text{-Circ}} = \begin{pmatrix} t_1 & & & 0 \\ \vdots & t_1 & & \\ t_d & \vdots & \ddots & \\ 1 & t_d & & t_1 \\ & 1 & \ddots & \vdots \\ & & \ddots & t_d \\ 0 & & & 1 \end{pmatrix}$$

A New Matrix Distribution With $\ell > k+1$

(k,d)-Circ: A compact hard matrix distribution with $\ell > k+1$

$$A_{(k,d)\text{-Circ}} = \begin{pmatrix} t_1 & & & 0 \\ \vdots & t_1 & & \\ t_d & \vdots & \ddots & \\ 1 & t_d & & t_1 \\ & 1 & \ddots & \vdots \\ & & \ddots & t_d \\ 0 & & & 1 \end{pmatrix}$$

- Optimal representation size for hard $(k+d) \times k$ polynomial matrix distributions of degree 1
- Application: Compact public key structure preserving commitments to vectors (see paper)

Generic Hardness of (k, d)-Circ

$A(\boldsymbol{t})$ has a constant nonzero k-minor (The "easy case" of the Determinant Criterion for $\ell > k + 1$ in [Herold2014])

Generic Hardness of (k, d)-Circ

$A(\boldsymbol{t})$ has a constant nonzero k-minor (The "easy case" of the Determinant Criterion for $\ell > k+1$ in [Herold2014])

The principal ideal $(\mathfrak{d})$ used in the case $\ell = k+1$ is replaced by the ideal $\mathfrak{I}$ generated by all the $(k+1)$-minors of $(A(\boldsymbol{t})\|\boldsymbol{z})$.

Generic Hardness of (k, d)-Circ

$A(\boldsymbol{t})$ has a constant nonzero k-minor (The "easy case" of the Determinant Criterion for $\ell > k+1$ in [Herold2014])

The principal ideal $(\mathfrak{d})$ used in the case $\ell = k+1$ is replaced by the ideal $\mathfrak{I}$ generated by all the $(k+1)$-minors of $(A(\boldsymbol{t})\|\boldsymbol{z})$.

Only polynomials $\mathfrak{p}$ in $\mathfrak{I}$ can be used successfully by a solver of (k, d)-Circ-MDDH.

Generic Hardness of (k, d)-Circ

$A(\boldsymbol{t})$ has a constant nonzero k-minor (The "easy case" of the Determinant Criterion for $\ell > k+1$ in [Herold2014])

The principal ideal $(\mathfrak{d})$ used in the case $\ell = k+1$ is replaced by the ideal $\mathfrak{I}$ generated by all the $(k+1)$-minors of $(A(\boldsymbol{t})\|\boldsymbol{z})$.

Only polynomials $\mathfrak{p}$ in $\mathfrak{I}$ can be used successfully by a solver of (k, d)-Circ-MDDH.

We prove that the set of $(k+1)$-minors of $(A(\boldsymbol{t})|\boldsymbol{z})$ for (k, d)-Circ is a Gröbner basis of $\mathfrak{I}$, and all minors have total degree $k+1$. Then, no nonzero polynomial of degree $\leq k$ exist in $\mathfrak{I}$.

Optimal Compactness of (k, d)-Circ

Theorem

Any hard polynomial matrix distribution $\mathcal{D}^{A}_{\ell,k}$ of degree 1, has at least $\ell - k$ parameters.

Optimal Compactness of (k, d)-Circ

Theorem

Any hard polynomial matrix distribution $\mathcal{D}^A_{\ell,k}$ of degree 1, has at least $\ell - k$ parameters.

If $d < \ell - k$: apply gaussian row elimination with scalar coefficients to the matrix $A(\boldsymbol{t}) \leftarrow \mathcal{D}^f_{\ell,k}$ to put at least $\ell - (d+1) \geq k$ zeros in the first column.

There exists an invertible matrix $L \in GL_\ell(\mathbb{Z}_q)$ such that $LA(\boldsymbol{t})$ has an identically zero k-minor.

$LA(\boldsymbol{t})$ defines an easy MDDH problem. Therefore, $\mathcal{D}_{\ell,k}$-MDDH is also easy.

The Kernel Matrix Diffie-Hellman Assumption

Carla Ràfols[1], Paz Morillo[2] and Jorge L. Villar[2]

[1] Universitat Pompeu Fabra (UPF) Spain

[2] Universitat Politècnica de Catalunya (UPC) Spain

MAK

Matemática Aplicada a la Criptografía

Asiacrypt 2016, Hanoi, 8 Dec 2016

The End!