KDM-Security *via* Homomorphic Smooth Projective Hashing

Hoeteck Wee

ENS, Paris

“ $\mathbf{enc}_{\mathrm{pk}}(\mathrm{sk})$ ”

“ $\mathbf{enc}_{pk}(sk)$ ”

key-dependent message security. **[Black Rogaway Shrimpton 02]**

- applications: formal methods **[Adão Bana Herzog Scedrov 05]**, credentials **[Camenisch Lysyanskaya 01]**, fully homomorphic encryption **[Gentry 09]**

“ $\mathbf{enc}_{\mathsf{pk}}(\mathsf{sk})$ ”

key-dependent message security. **[Black Rogaway Shrimpton 02]**

- many constructions [**Boneh Halevi Hamburg Ostrovsky 08, Applebaum Cash Peikert Sahai 09, Brakerski Goldwasser 10, Brakerski Vaikuntanathan 11, Barak Haitner Hofheinz Ishai 10, Brakerski Goldwasser Kalai 11, Malkin Teranishi Yung 11, Applebaum 11, ...**]

“ $\mathbf{enc}_{pk}(sk)$ ”

key-dependent message security. [**Black Rogaway Shrimpton 02**]

- many constructions [**Boneh Halevi Hamburg Ostrovsky 08, Applebaum Cash Peikert Sahai 09, Brakerski Goldwasser 10, Brakerski Vaikuntanathan 11, Barak Haitner Hofheinz Ishai 10, Brakerski Goldwasser Kalai 11, Malkin Teranishi Yung 11, Applebaum 11, ...**]

this work. unifying framework with a simple proof of security

Projective Hashing

definition. **projective hash function** for $\mathcal{G} \supseteq \mathcal{G}_{\mathsf{y}}$ **[Cramer Shoup 02]**

– family $\Lambda_{\mathsf{sk}}(C \in \mathcal{G})$ indexed by sk

Projective Hashing

definition. projective hash function for $\mathcal{G} \supseteq \mathcal{G}_{\mathsf{y}}$ **[Cramer Shoup 02]**

- family $\Lambda_{\mathsf{sk}}(C \in \mathcal{G})$ indexed by sk **+** map μ
- (**projective**) $\Lambda_{\mathsf{sk}}(C \in \mathcal{G}_{\mathsf{y}})$ determined given $\mu(\mathsf{sk})$

  where μ is lossy

Projective Hashing

definition. **projective hash function** for $\mathcal{G} \supseteq \mathcal{G}_{\mathsf{y}}$ **[Cramer Shoup 02]**

- family $\Lambda_{\mathsf{sk}}(C \in \mathcal{G})$ indexed by sk **+** map μ
- (**projective**) $\Lambda_{\mathsf{sk}}(C \in \mathcal{G}_{\mathsf{y}}) = \mathbf{pub}(\mu(\mathsf{sk}), C, r)$ witness r

Projective Hashing

definition. **projective hash function** for $\mathcal{G} \supseteq \mathcal{G}_{\mathsf{y}}$ **[Cramer Shoup 02]**

- family $\Lambda_{\mathsf{sk}}(C \in \mathcal{G})$ indexed by sk **+** map μ
- (**projective**) $\Lambda_{\mathsf{sk}}(C \in \mathcal{G}_{\mathsf{y}}) = \textbf{pub}(\mu(\mathsf{sk}), C, r)$
- (**smoothness**) $\Lambda_{\mathsf{sk}}(C \notin \mathcal{G}_{\mathsf{y}})$ random given $\mu(\mathsf{sk})$

Projective Hashing

definition. **projective hash function** for $\mathcal{G} \supseteq \mathcal{G}_{\mathsf{y}}$ **[Cramer Shoup 02]**

- family $\Lambda_{\mathsf{sk}}(C \in \mathcal{G})$ indexed by sk **+** map μ
- (**projective**) $\Lambda_{\mathsf{sk}}(C \in \mathcal{G}_{\mathsf{y}}) = \mathbf{pub}(\mu(\mathsf{sk}), C, r)$
- (**smoothness**) $\Lambda_{\mathsf{sk}}(C \xleftarrow{\mathsf{r}} \mathcal{G})$ random given $\mu(\mathsf{sk}), C$

Projective Hashing

definition. **projective hash function** for $\mathcal{G} \supseteq \mathcal{G}_{\mathsf{y}}$ **[Cramer Shoup 02]**

- family $\Lambda_{\mathsf{sk}}(C \in \mathcal{G})$ indexed by sk **+** map μ
- (**projective**) $\Lambda_{\mathsf{sk}}(C \in \mathcal{G}_{\mathsf{y}}) = \mathbf{pub}(\mu(\mathsf{sk}), C, r)$
- (**smoothness**) $\Lambda_{\mathsf{sk}}(C \xleftarrow{\mathsf{r}} \mathcal{G})$ random given $\mu(\mathsf{sk}), C$

subgroup assumption. uniform$(\mathcal{G}_{\mathsf{y}}) \approx_c$ uniform$(\mathcal{G})$

Projective Hashing

definition. **projective hash function** for $\mathcal{G} \supseteq \mathcal{G}_{\mathsf{y}}$ **[Cramer Shoup 02]**

- family $\Lambda_{\mathsf{sk}}(C \in \mathcal{G})$ indexed by sk **+** map μ
- (**projective**) $\Lambda_{\mathsf{sk}}(C \in \mathcal{G}_{\mathsf{y}}) = \mathbf{pub}(\mu(\mathsf{sk}), C, r)$
- (**smoothness**) $\Lambda_{\mathsf{sk}}(C \xleftarrow{r} \mathcal{G})$ random given $\mu(\mathsf{sk}), C$

DDH instantiation. **[Cramer Shoup 98]**

- $\mathsf{pp} = (g, g^a), \mathcal{G}_{\mathsf{y}} = (g^r, g^{ar}) \subset \mathcal{G} = G^2$
- DDH assumption $\Leftrightarrow$ uniform$(\mathcal{G}_{\mathsf{y}}) \approx_c$ uniform$(\mathcal{G})$

Projective Hashing

definition. **projective hash function** for $\mathcal{G} \supseteq \mathcal{G}_{\mathsf{y}}$ **[Cramer Shoup 02]**

- family $\Lambda_{\mathsf{sk}}(C \in \mathcal{G})$ indexed by sk **+** map μ
- (**projective**) $\Lambda_{\mathsf{sk}}(C \in \mathcal{G}_{\mathsf{y}}) = \mathbf{pub}(\mu(\mathsf{sk}), C, r)$
- (**smoothness**) $\Lambda_{\mathsf{sk}}(C \xleftarrow{\mathsf{r}} \mathcal{G})$ random given $\mu(\mathsf{sk}), C$

DDH instantiation. **[Cramer Shoup 98]**

- $\mathsf{pp} = (g, g^a), \mathcal{G}_{\mathsf{y}} = (g^r, g^{ar}) \subset \mathcal{G} = G^2$
- $\Lambda_{(x,y)}(c_0, c_1) = c_0^x c_1^y$

Projective Hashing

definition. **projective hash function** for $\mathcal{G} \supseteq \mathcal{G}_{\mathsf{y}}$ **[Cramer Shoup 02]**

- family $\Lambda_{\mathsf{sk}}(C \in \mathcal{G})$ indexed by sk **+** map μ
- (**projective**) $\Lambda_{\mathsf{sk}}(C \in \mathcal{G}_{\mathsf{y}}) = \mathbf{pub}(\mu(\mathsf{sk}), C, r)$
- (**smoothness**) $\Lambda_{\mathsf{sk}}(C \xleftarrow{\mathsf{r}} \mathcal{G})$ random given $\mu(\mathsf{sk}), C$

DDH instantiation. **[Cramer Shoup 98]**

- $\mathsf{pp} = (g, g^a), \mathcal{G}_{\mathsf{y}} = (g^r, g^{ar}) \subset \mathcal{G} = G^2$
- $\Lambda_{(x,y)}(c_0, c_1) = c_0^x c_1^y$ i.e. $\Lambda_{(x,y)}(g^r, g^{ar}) = (g^{x+ay})^r$

Projective Hashing

definition. **projective hash function** for $\mathcal{G} \supseteq \mathcal{G}_{\mathsf{y}}$ **[Cramer Shoup 02]**

- family $\Lambda_{\mathsf{sk}}(C \in \mathcal{G})$ indexed by sk **+** map μ
- (**projective**) $\Lambda_{\mathsf{sk}}(C \in \mathcal{G}_{\mathsf{y}}) = \mathbf{pub}(\mu(\mathsf{sk}), C, r)$
- (**smoothness**) $\Lambda_{\mathsf{sk}}(C \overset{r}{\leftarrow} \mathcal{G})$ random given $\mu(\mathsf{sk}), C$

DDH instantiation. **[Cramer Shoup 98]**

- $\mathsf{pp} = (g, g^a), \mathcal{G}_{\mathsf{y}} = (g^r, g^{ar}) \subset \mathcal{G} = G^2$
- $\Lambda_{(x,y)}(c_0, c_1) = c_0^x c_1^y$ i.e. $\Lambda_{(x,y)}(g^r, g^{ar}) = (g^{x+ay})^r$
- $\mu(x, y) = g^{x+ay}$

Projective Hashing

definition. **projective hash function** for $\mathcal{G} \supseteq \mathcal{G}_{\mathsf{y}}$ **[Cramer Shoup 02]**

- family $\Lambda_{\mathsf{sk}}(C \in \mathcal{G})$ indexed by sk **+** map μ
- (**projective**) $\Lambda_{\mathsf{sk}}(C \in \mathcal{G}_{\mathsf{y}}) = \mathbf{pub}(\mu(\mathsf{sk}), C, r)$
- (**smoothness**) $\Lambda_{\mathsf{sk}}(C \xleftarrow{r} \mathcal{G})$ random given $\mu(\mathsf{sk}), C$

DDH instantiation. **[Cramer Shoup 98]**

- $\mathsf{pp} = (g, g^a), \mathcal{G}_{\mathsf{y}} = (g^r, g^{ar}) \subset \mathcal{G} = G^2$
- $\Lambda_{(x,y)}(c_0, c_1) = c_0^x c_1^y$ i.e. $\Lambda_{(x,y)}(g^r, g^{ar}) = (g^{x+ay})^r$
- $\mu(x, y) = g^{x+ay}$
- $\Lambda_{(x,y)}(g^r, g^{ar'}) = g^{(xr+ayr')}$ random given $x + ay$ and $r \neq r'$

Projective Hashing

definition. **projective hash function** for $\mathcal{G} \supseteq \mathcal{G}_{\mathsf{y}}$ **[Cramer Shoup 02]**

- family $\Lambda_{\mathsf{sk}}(C \in \mathcal{G})$ indexed by sk **+** map μ
- (**projective**) $\Lambda_{\mathsf{sk}}(C \in \mathcal{G}_{\mathsf{y}}) = \mathbf{pub}(\mu(\mathsf{sk}), C, r)$
- (**smoothness**) $\Lambda_{\mathsf{sk}}(C \xleftarrow{\mathsf{r}} \mathcal{G})$ random given $\mu(\mathsf{sk}), C$

cpa-secure encryption. $\Lambda_{\mathsf{sk}}(\cdot)$ as one-time pad

- $\mathbf{gen}(\mathsf{pp}) : (\mathsf{pk}, \mathsf{sk}), \mathsf{pk} = \mu(\mathsf{sk})$
- $\mathbf{enc}_{\mathsf{pk}}(m) : (C, \underbrace{\Lambda_{\mathsf{sk}}(C)}_{\mathbf{pub}(\mathsf{pk}, C, r)} \cdot m), C \xleftarrow{\mathsf{r}} \mathcal{G}_{\mathsf{y}}$

Projective Hashing

definition. **projective hash function** for $\mathcal{G} \supseteq \mathcal{G}_{\mathsf{y}}$ **[Cramer Shoup 02]**

- family $\Lambda_{\mathsf{sk}}(C \in \mathcal{G})$ indexed by sk **+** map μ
- (**projective**) $\Lambda_{\mathsf{sk}}(C \in \mathcal{G}_{\mathsf{y}}) = \textbf{pub}(\mu(\mathsf{sk}), C, r)$
- (**smoothness**) $\Lambda_{\mathsf{sk}}(C \xleftarrow{\mathsf{r}} \mathcal{G})$ random given $\mu(\mathsf{sk}), C$

cpa-secure encryption. $\Lambda_{\mathsf{sk}}(\cdot)$ as one-time pad

- $\textbf{gen}(\mathsf{pp}) : (\mathsf{pk}, \mathsf{sk}), \mathsf{pk} = \mu(\mathsf{sk})$
- $\textbf{enc}_{\mathsf{pk}}(m) : (C,\ \Lambda_{\mathsf{sk}}(C)\ \cdot\ m), C \xleftarrow{\mathsf{r}} \mathcal{G}_{\mathsf{y}}$
- $\textbf{dec}_{\mathsf{sk}}(C, \psi) : \Lambda_{\mathsf{sk}}(C)^{-1} \cdot \psi$

Projective Hashing

definition. **projective hash function** for $\mathcal{G} \supseteq \mathcal{G}_{\mathsf{y}}$ **[Cramer Shoup 02]**

- family $\Lambda_{\mathsf{sk}}(C \in \mathcal{G})$ indexed by sk **+** map μ
- (**projective**) $\Lambda_{\mathsf{sk}}(C \in \mathcal{G}_{\mathsf{y}}) = \mathbf{pub}(\mu(\mathsf{sk}), C, r)$
- (**smoothness**) $\Lambda_{\mathsf{sk}}(C \xleftarrow{\mathsf{r}} \mathcal{G})$ random given $\mu(\mathsf{sk}), C$

cpa-secure encryption. $\Lambda_{\mathsf{sk}}(\cdot)$ as one-time pad

- $\mathbf{gen}(\mathsf{pp}) : (\mathsf{pk}, \mathsf{sk}), \mathsf{pk} = \mu(\mathsf{sk})$
- $\mathbf{enc}_{\mathsf{pk}}(m) : (C, \ \Lambda_{\mathsf{sk}}(C) \ \cdot \ m), C \xleftarrow{\mathsf{r}} \mathcal{G}_{\mathsf{y}}$

subgroup + smoothness $\Rightarrow$ cpa-security

Projective Hashing

definition. **projective hash function** for $\mathcal{G} \supseteq \mathcal{G}_{\mathsf{y}}$ **[Cramer Shoup 02]**

- family $\Lambda_{\mathsf{sk}}(C \in \mathcal{G})$ indexed by sk **+** map μ
- (**projective**) $\Lambda_{\mathsf{sk}}(C \in \mathcal{G}_{\mathsf{y}}) = \mathbf{pub}(\mu(\mathsf{sk}), C, r)$
- (**smoothness**) $\Lambda_{\mathsf{sk}}(C \xleftarrow{\mathsf{r}} \mathcal{G})$ random given $\mu(\mathsf{sk}), C$

cpa-secure encryption. $\Lambda_{\mathsf{sk}}(\cdot)$ as one-time pad

- $\mathbf{gen}(\mathsf{pp}) : (\mathsf{pk}, \mathsf{sk}), \mathsf{pk} = \mu(\mathsf{sk})$
- $\mathbf{enc}_{\mathsf{pk}}(m) : (C,\ \Lambda_{\mathsf{sk}}(C) \cdot m), C \xleftarrow{\mathsf{r}} \mathcal{G}_{\mathsf{y}}$

subgroup + smoothness $\Rightarrow$ cpa-security

$$(C,\ \Lambda_{\mathsf{sk}}(C))_{C \xleftarrow{\mathsf{r}} \mathcal{G}_{\mathsf{y}}} \approx_c (C,\ \Lambda_{\mathsf{sk}}(C))_{C \xleftarrow{\mathsf{r}} \mathcal{G}}$$

Projective Hashing

definition. **projective hash function** for $\mathcal{G} \supseteq \mathcal{G}_{\mathsf{y}}$ **[Cramer Shoup 02]**

- family $\Lambda_{\mathsf{sk}}(C \in \mathcal{G})$ indexed by sk **+** map μ
- (**projective**) $\Lambda_{\mathsf{sk}}(C \in \mathcal{G}_{\mathsf{y}}) = \mathbf{pub}(\mu(\mathsf{sk}), C, r)$
- (**smoothness**) $\Lambda_{\mathsf{sk}}(C \xleftarrow{\mathsf{r}} \mathcal{G})$ random given $\mu(\mathsf{sk}), C$

cpa-secure encryption. $\Lambda_{\mathsf{sk}}(\cdot)$ as one-time pad

- $\mathbf{gen}(\mathsf{pp}) : (\mathsf{pk}, \mathsf{sk}), \mathsf{pk} = \mu(\mathsf{sk})$
- $\mathbf{enc}_{\mathsf{pk}}(m) : (C,\ \Lambda_{\mathsf{sk}}(C)\ \cdot\ m), C \xleftarrow{\mathsf{r}} \mathcal{G}_{\mathsf{y}}$

subgroup + **smoothness** $\Rightarrow$ cpa-security

$$(C,\ \Lambda_{\mathsf{sk}}(C))_{C \xleftarrow{\mathsf{r}} \mathcal{G}_{\mathsf{y}}} \approx_c (C,\ \Lambda_{\mathsf{sk}}(C))_{C \xleftarrow{\mathsf{r}} \mathcal{G}} \approx_s (C,\ \text{random})_{C \xleftarrow{\mathsf{r}} \mathcal{G}}$$

Projective Hashing

definition. **projective hash function** for $\mathcal{G} \supseteq \mathcal{G}_{\mathsf{y}}$ **[Cramer Shoup 02]**

- family $\Lambda_{\mathsf{sk}}(C \in \mathcal{G})$ indexed by sk **+** map μ
- (**projective**) $\Lambda_{\mathsf{sk}}(C \in \mathcal{G}_{\mathsf{y}}) = \mathbf{pub}(\mu(\mathsf{sk}), C, r)$
- (**smoothness**) $\Lambda_{\mathsf{sk}}(C \xleftarrow{r} \mathcal{G})$ random given $\mu(\mathsf{sk}), C$

cpa-secure encryption. $\Lambda_{\mathsf{sk}}(\cdot)$ as one-time pad

- $\mathbf{gen}(\mathsf{pp}) : (\mathsf{pk}, \mathsf{sk}), \mathsf{pk} = \mu(\mathsf{sk})$
- $\mathbf{enc}_{\mathsf{pk}}(m) : (C,\ \Lambda_{\mathsf{sk}}(C) \cdot m), C \xleftarrow{r} \mathcal{G}_{\mathsf{y}}$

subgroup + smoothness $\Rightarrow$ **cpa-security**

$$(C,\ \Lambda_{\mathsf{sk}}(C))_{C \xleftarrow{r} \mathcal{G}_{\mathsf{y}}} \approx_c (C,\ \Lambda_{\mathsf{sk}}(C))_{C \xleftarrow{r} \mathcal{G}} \approx_s (C,\ \text{random})_{C \xleftarrow{r} \mathcal{G}}$$

KDM security

definition. $(\textbf{gen}, \textbf{enc}, \textbf{dec})$ is **KDM secure** w.r.t. $\mathcal{F}$ if

$$\textbf{sim}(\mathsf{pk}, f) \approx_c \textbf{enc}_{\mathsf{pk}}(f(\mathsf{sk})) \text{ for all } f \in \mathcal{F}$$

KDM security

definition. (**gen**, **enc**, **dec**) is **KDM secure** w.r.t. $\mathcal{F}$ if

$\mathbf{sim}(\mathsf{pk}, f) \approx_c \mathbf{enc}_{\mathsf{pk}}(f(\mathsf{sk}))$ for all $f \in \mathcal{F}$

e.g. $f(\mathsf{sk}) = \mathsf{sk}_i$ or $f(\mathsf{sk}) = 1 - \mathsf{sk}_i$ or $f(\mathsf{sk}) = \mathsf{sk}_2 + \mathsf{sk}_5 + \mathsf{sk}_7$

KDM security

definition. $(\textbf{gen}, \textbf{enc}, \textbf{dec})$ is **KDM secure** w.r.t. $\mathcal{F}$ if

$$\textbf{sim}(\mathsf{pk}, f) \approx_c \textbf{enc}_{\mathsf{pk}}(f(\mathsf{sk})) \text{ for all } f \in \mathcal{F}$$

theorem. CPA scheme is **KDM secure**

KDM security

definition. ($\mathbf{gen}, \mathbf{enc}, \mathbf{dec}$) is **KDM secure** w.r.t. $\mathcal{F}$ if

$\mathbf{sim}(\mathsf{pk}, f) \approx_c \mathbf{enc}_{\mathsf{pk}}(f(\mathsf{sk}))$ for all $f \in \mathcal{F}$

theorem. CPA scheme is **KDM secure** ,

if $\Lambda_{\mathsf{sk}}(\cdot)$ is homomorphic i.e. $\Lambda_{\mathsf{sk}}(C_0 \cdot C_1) = \Lambda_{\mathsf{sk}}(C_0) \cdot \Lambda_{\mathsf{sk}}(C_1)$

KDM security

definition. $(\textbf{gen}, \textbf{enc}, \textbf{dec})$ is **KDM secure** w.r.t. $\mathcal{F}$ if

$\textbf{sim}(\mathsf{pk}, f) \approx_c \textbf{enc}_{\mathsf{pk}}(f(\mathsf{sk}))$ for all $f \in \mathcal{F}$

theorem. CPA scheme is **KDM secure** ,

if $\Lambda_{\mathsf{sk}}(\cdot)$ is homomorphic

1. $\forall e \in \mathcal{G}$, subgroup $\Rightarrow (\, C \,)_{C \xleftarrow{r} \mathcal{G}_{\mathsf{y}}} \approx_c (\, C \cdot e \,)_{C \xleftarrow{r} \mathcal{G}_{\mathsf{y}}}$

KDM security

definition. (**gen**, **enc**, **dec**) is **KDM secure** w.r.t. $\mathcal{F}$ if

sim(pk, f) $\approx_c$ **enc**$_{\mathsf{pk}}$(f(sk)) for all $f \in \mathcal{F}$

theorem. CPA scheme is **KDM secure** ,

if $\Lambda_{\mathsf{sk}}(\cdot)$ is homomorphic

1. $\forall e \in \mathcal{G}$, subgroup $\Rightarrow (\, C \,)_{C \xleftarrow{r} \mathcal{G}_y} \approx_c (\, C \cdot e \,)_{C \xleftarrow{r} \mathcal{G}_y}$

2.

$$(\, C, \Lambda_{\mathsf{sk}}(C) \,)_{C \xleftarrow{r} \mathcal{G}_y} \approx_c (\, C \cdot e, \Lambda_{\mathsf{sk}}(C \cdot e) \,)_{C \xleftarrow{r} \mathcal{G}_y}$$

KDM security

definition. (**gen**, **enc**, **dec**) is **KDM secure** w.r.t. $\mathcal{F}$ if

sim(pk, f) $\approx_c$ $\mathbf{enc}_{\mathsf{pk}}(f(\mathsf{sk}))$ for all $f \in \mathcal{F}$

theorem. CPA scheme is **KDM secure** ,

if $\Lambda_{\mathsf{sk}}(\cdot)$ is homomorphic

1. $\forall e \in \mathcal{G}$, subgroup $\Rightarrow$ $(\, C \,)_{C \xleftarrow{r} \mathcal{G}_y} \approx_c (\, C \cdot e \,)_{C \xleftarrow{r} \mathcal{G}_y}$

2.

$$(\, C \cdot e^{-1}, \Lambda_{\mathsf{sk}}(C) \,)_{C \xleftarrow{r} \mathcal{G}_y} \qquad \approx_c \qquad (\, C, \Lambda_{\mathsf{sk}}(C \cdot e) \,)_{C \xleftarrow{r} \mathcal{G}_y}$$

KDM security

definition. $(\mathbf{gen}, \mathbf{enc}, \mathbf{dec})$ is **KDM secure** w.r.t. $\mathcal{F}$ if

$\mathbf{sim}(\mathsf{pk}, f) \approx_c \mathbf{enc}_{\mathsf{pk}}(f(\mathsf{sk}))$ for all $f \in \mathcal{F}$

theorem. CPA scheme is **KDM secure** ,

if $\Lambda_{\mathsf{sk}}(\cdot)$ is **homomorphic**

1. $\forall e \in \mathcal{G}$, subgroup $\Rightarrow (\, C \,)_{C \xleftarrow{r} \mathcal{G}_y} \approx_c (\, C \cdot e \,)_{C \xleftarrow{r} \mathcal{G}_y}$

2.

$$(\, C \cdot e^{-1}, \Lambda_{\mathsf{sk}}(C) \,)_{C \xleftarrow{r} \mathcal{G}_y} \quad \approx_c \quad (\, C, \Lambda_{\mathsf{sk}}(C) \cdot \Lambda_{\mathsf{sk}}(e) \,)_{C \xleftarrow{r} \mathcal{G}_y}$$

KDM security

definition. (**gen**, **enc**, **dec**) is **KDM secure** w.r.t. $\mathcal{F}$ if

$$\textbf{sim}(\mathsf{pk}, f) \approx_c \textbf{enc}_{\mathsf{pk}}(f(\mathsf{sk})) \text{ for all } f \in \mathcal{F}$$

theorem. CPA scheme is **KDM secure** ,

if $\Lambda_{\mathsf{sk}}(\cdot)$ is homomorphic

1. $\forall e \in \mathcal{G}$, subgroup $\Rightarrow (\, C \,)_{C \xleftarrow{r} \mathcal{G}_y} \approx_c (\, C \cdot e \,)_{C \xleftarrow{r} \mathcal{G}_y}$

2.

$$(\, C \cdot e^{-1}, \Lambda_{\mathsf{sk}}(C) \,)_{C \xleftarrow{r} \mathcal{G}_y} \approx_c (\, \underbrace{C, \Lambda_{\mathsf{sk}}(C) \cdot \Lambda_{\mathsf{sk}}(e)}_{\textbf{enc}_{\mathsf{pk}}(\Lambda_{\mathsf{sk}}(e))} \,)_{C \xleftarrow{r} \mathcal{G}_y}$$

KDM security

definition. (**gen**, **enc**, **dec**) is **KDM secure** w.r.t. $\mathcal{F}$ if

sim(pk,f) $\approx_c$ **enc**$_{\mathsf{pk}}$(f(sk)) for all $f \in \mathcal{F}$

theorem. CPA scheme is **KDM secure** ,

if $\Lambda_{\mathsf{sk}}(\cdot)$ is homomorphic

1. $\forall e \in \mathcal{G}$, subgroup $\Rightarrow (\, C \,)_{C \xleftarrow{r} \mathcal{G}_y} \approx_c (\, C \cdot e \,)_{C \xleftarrow{r} \mathcal{G}_y}$

2.

$$(\, C \cdot e^{-1}, \underbrace{\Lambda_{\mathsf{sk}}(C)}_{\textbf{pub}(\mathsf{pk},C)} \,)_{C \xleftarrow{r} \mathcal{G}_y} \approx_c (\, \underbrace{C, \Lambda_{\mathsf{sk}}(C) \cdot \Lambda_{\mathsf{sk}}(e)}_{\textbf{enc}_{\mathsf{pk}}(\Lambda_{\mathsf{sk}}(e))} \,)_{C \xleftarrow{r} \mathcal{G}_y}$$

KDM security

definition. (**gen**, **enc**, **dec**) is **KDM secure** w.r.t. $\mathcal{F}$ if

$\textbf{sim}(\text{pk}, f) \approx_c \textbf{enc}_{\text{pk}}(f(\text{sk}))$ for all $f \in \mathcal{F}$

theorem. CPA scheme is **KDM secure** w.r.t. $\{\text{sk} \mapsto \Lambda_{\text{sk}}(e)\}_{e \in \mathcal{G}}$,

if $\Lambda_{\text{sk}}(\cdot)$ is homomorphic

1. $\forall e \in \mathcal{G}$, subgroup $\Rightarrow (\, C \,)_{C \xleftarrow{r} \mathcal{G}_y} \approx_c (\, C \cdot e \,)_{C \xleftarrow{r} \mathcal{G}_y}$

2. $$(\, C \cdot e^{-1}, \underbrace{\Lambda_{\text{sk}}(C)}_{\textbf{pub}(\text{pk}, C)} \,)_{C \xleftarrow{r} \mathcal{G}_y} \quad \approx_c \quad (\, \underbrace{C, \Lambda_{\text{sk}}(C) \cdot \Lambda_{\text{sk}}(e)}_{\textbf{enc}_{\text{pk}}(\Lambda_{\text{sk}}(e))} \,)_{C \xleftarrow{r} \mathcal{G}_y}$$

KDM security

definition. (**gen**, **enc**, **dec**) is **KDM secure** w.r.t. $\mathcal{F}$ if

sim(pk, f) $\approx_c$ $\mathbf{enc}_{\mathsf{pk}}(f(\mathsf{sk}))$ for all $f \in \mathcal{F}$

theorem. CPA scheme is **KDM secure** w.r.t. $\{\mathsf{sk} \mapsto \Lambda_{\mathsf{sk}}(e)\}_{e \in \mathcal{G}}$,

if $\Lambda_{\mathsf{sk}}(\cdot)$ is homomorphic

1. $\forall e \in \mathcal{G}$, subgroup $\Rightarrow$ $(\, C \,)_{C \xleftarrow{r} \mathcal{G}_y} \approx_c (\, C \cdot e \,)_{C \xleftarrow{r} \mathcal{G}_y}$

2.

$$(\, C \cdot e^{-1}, \underbrace{\Lambda_{\mathsf{sk}}(C)}_{\mathbf{pub}(\mathsf{pk}, C)} \,)_{C \xleftarrow{r} \mathcal{G}_y} \quad \approx_c \quad (\, \underbrace{C, \Lambda_{\mathsf{sk}}(C) \cdot \Lambda_{\mathsf{sk}}(e)}_{\mathbf{enc}_{\mathsf{pk}}(\Lambda_{\mathsf{sk}}(e))} \,)_{C \xleftarrow{r} \mathcal{G}_y}$$

note. only use smoothness for CPA security.

Instantiations

theorem. CPA scheme is **KDM secure** w.r.t. $\{\mathsf{sk} \mapsto \Lambda_{\mathsf{sk}}(e)\}_{e \in \mathcal{G}}$,

if $\Lambda_{\mathsf{sk}}(\cdot)$ is homomorphic

Instantiations

theorem. CPA scheme is **KDM secure** w.r.t. $\{\mathsf{sk} \mapsto \Lambda_{\mathsf{sk}}(e)\}_{e \in \mathcal{G}}$,

if $\Lambda_{\mathsf{sk}}(\cdot)$ is homomorphic

DDH instantiation I. **[Cramer Shoup 98]**

$$\mathsf{sk} = (x, y) \in \mathbb{Z}_q^2, \quad \Lambda_{(x,y)}(c_0, c_1) = c_0^x c_1^y, \quad \Lambda_{(x,y)}(g, 1) = g^x$$

Instantiations

theorem. CPA scheme is **KDM secure** w.r.t. $\{\mathsf{sk} \mapsto \Lambda_{\mathsf{sk}}(e)\}_{e \in \mathcal{G}}$,

if $\Lambda_{\mathsf{sk}}(\cdot)$ is homomorphic

DDH instantiation I. [Cramer Shoup 98]

$$\mathsf{sk} = (x, y) \in \mathbb{Z}_q^2, \quad \Lambda_{(x,y)}(c_0, c_1) = c_0^x c_1^y, \quad \Lambda_{(x,y)}(g, 1) = g^x$$

DDH instantiation II. [Boneh Halevi Hamburg Ostrovsky 08]

– $\mathsf{sk} = (g^{x_1}, \ldots, g^{x_\ell}), x_1, \ldots, x_\ell \in \{0, 1\}, \ell \approx 3 \log q$

Instantiations

theorem. CPA scheme is **KDM secure** w.r.t. $\{\mathsf{sk} \mapsto \Lambda_{\mathsf{sk}}(e)\}_{e \in \mathcal{G}}$,

if $\Lambda_{\mathsf{sk}}(\cdot)$ is homomorphic

DDH instantiation I. **[Cramer Shoup 98]**

$$\mathsf{sk} = (x, y) \in \mathbb{Z}_q^2, \quad \Lambda_{(x,y)}(c_0, c_1) = c_0^x c_1^y, \quad \Lambda_{(x,y)}(g, 1) = g^x$$

DDH instantiation II. **[Boneh Halevi Hamburg Ostrovsky 08]**

- $\mathsf{sk} = (g^{x_1}, \ldots, g^{x_\ell}), x_1, \ldots, x_\ell \in \{0, 1\}, \ell \approx 3 \log q$
- $\mathsf{pp} = (g_1, \ldots, g_\ell), \mathcal{G}_{\mathsf{y}} = (g_1^r, \ldots, g_\ell^r) \subset \mathcal{G} = G^\ell$
- $\Lambda_{(x_1, \ldots, x_\ell)}(c_1, \ldots, c_\ell) = c_1^{x_1} \cdots c_\ell^{x_\ell}$

Instantiations

theorem. CPA scheme is **KDM secure** w.r.t. $\{\mathsf{sk} \mapsto \Lambda_{\mathsf{sk}}(e)\}_{e \in \mathcal{G}}$, if $\Lambda_{\mathsf{sk}}(\cdot)$ is homomorphic

DDH instantiation I. **[Cramer Shoup 98]**

$$\mathsf{sk} = (x, y) \in \mathbb{Z}_q^2, \quad \Lambda_{(x,y)}(c_0, c_1) = c_0^x c_1^y, \quad \Lambda_{(x,y)}(g, 1) = g^x$$

DDH instantiation II. **[Boneh Halevi Hamburg Ostrovsky 08]**

- $\mathsf{sk} = (g^{x_1}, \ldots, g^{x_\ell}), x_1, \ldots, x_\ell \in \{0, 1\}, \ell \approx 3 \log q$
- $\mathsf{pp} = (g_1, \ldots, g_\ell), \mathcal{G}_{\mathsf{y}} = (g_1^r, \ldots, g_\ell^r) \subset \mathcal{G} = G^\ell$
- $\Lambda_{(x_1, \ldots, x_\ell)}(c_1, \ldots, c_\ell) = c_1^{x_1} \cdots c_\ell^{x_\ell}$
- $\Lambda_{(x_1, \ldots, x_\ell)}(g, 1, \ldots, 1) = g^{x_1}$

Instantiations

theorem. CPA scheme is **KDM secure** w.r.t. $\{\mathsf{sk} \mapsto \Lambda_{\mathsf{sk}}(e)\}_{e \in \mathcal{G}}$,

if $\Lambda_{\mathsf{sk}}(\cdot)$ is homomorphic

DDH instantiation I. [Cramer Shoup 98]

$$\mathsf{sk} = (x, y) \in \mathbb{Z}_q^2, \quad \Lambda_{(x,y)}(c_0, c_1) = c_0^x c_1^y, \quad \Lambda_{(x,y)}(g, 1) = g^x$$

DDH instantiation II. [Boneh Halevi Hamburg Ostrovsky 08]

- $\mathsf{sk} = (g^{x_1}, \ldots, g^{x_\ell}), x_1, \ldots, x_\ell \in \{0, 1\}, \ell \approx 3 \log q$
- $\mathsf{pp} = (g_1, \ldots, g_\ell), \mathcal{G}_{\mathsf{y}} = (g_1^r, \ldots, g_\ell^r) \subset \mathcal{G} = G^\ell$
- $\Lambda_{(x_1,\ldots,x_\ell)}(c_1, \ldots, c_\ell) = c_1^{x_1} \cdots c_\ell^{x_\ell}$
- $\Lambda_{(x_1,\ldots,x_\ell)}(g^{a_1}, \ldots, g^{a_\ell}) = g^{a_1 x_1 + \cdots + a_\ell x_\ell}$

Additional Results

1. instantiations from DCR, QR [**Brakerski Goldwasser 10**]

Additional Results

1. instantiations from DCR, QR **[Brakerski Goldwasser 10]**
2. fixed functions $f_1, \ldots, f_t$ **[Brakerski Goldwasser Kalai 11]**

– $\Lambda_{(x_1,\ldots,x_\ell)}(c_1, \ldots, c_{\ell+t}) = c_1^{x_1} \cdots c_\ell^{x_\ell} c_{\ell+1}^{f_1(\mathsf{sk})} \cdots c_{\ell+1}^{f_t(\mathsf{sk})}$

Additional Results

1. instantiations from DCR, QR **[Brakerski Goldwasser 10]**
2. fixed functions $f_1, \ldots, f_t$ **[Brakerski Goldwasser Kalai 11]**
   - $\Lambda_{(x_1,\ldots,x_\ell)}(c_1, \ldots, c_{\ell+t}) = c_1^{x_1} \cdots c_\ell^{x_\ell} c_{\ell+1}^{f_1(\mathsf{sk})} \cdots c_{\ell+1}^{f_t(\mathsf{sk})}$
3. UC-secure oblivious transfer **[Peikert Waters Vaikuntanathan 08]**

Additional Results

1. instantiations from DCR, QR **[Brakerski Goldwasser 10]**
2. fixed functions $f_1, \ldots, f_t$ **[Brakerski Goldwasser Kalai 11]**
   - $\Lambda_{(x_1,\ldots,x_\ell)}(c_1, \ldots, c_{\ell+t}) = c_1^{x_1} \cdots c_\ell^{x_\ell} c_{\ell+1}^{f_1(\mathsf{sk})} \cdots c_{\ell+1}^{f_t(\mathsf{sk})}$
3. UC-secure oblivious transfer **[Peikert Waters Vaikuntanathan 08]**

// thank you