Dual System Encryption Framework in Prime-Order Groups via Computational Pair Encodings

Nuttapong Attrapadung (Nuts)
AIST, Japan

Asiacrypt 2016
Hanoi, Vietnam, December 7, 2016

Our Main Result in One Slide

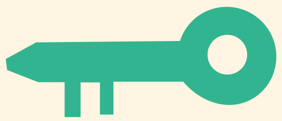
A Generic Framework for Fully Secure ABE in Prime-order Groups

Implies many first fully-secure&prime-order instantiations: ABE for regular languages, Short-ciphertext ABE, etc.

1 Introduction

Attribute Based Encryption (ABE) [SW05]

ABE for predicate R: X × Y → {0,1}



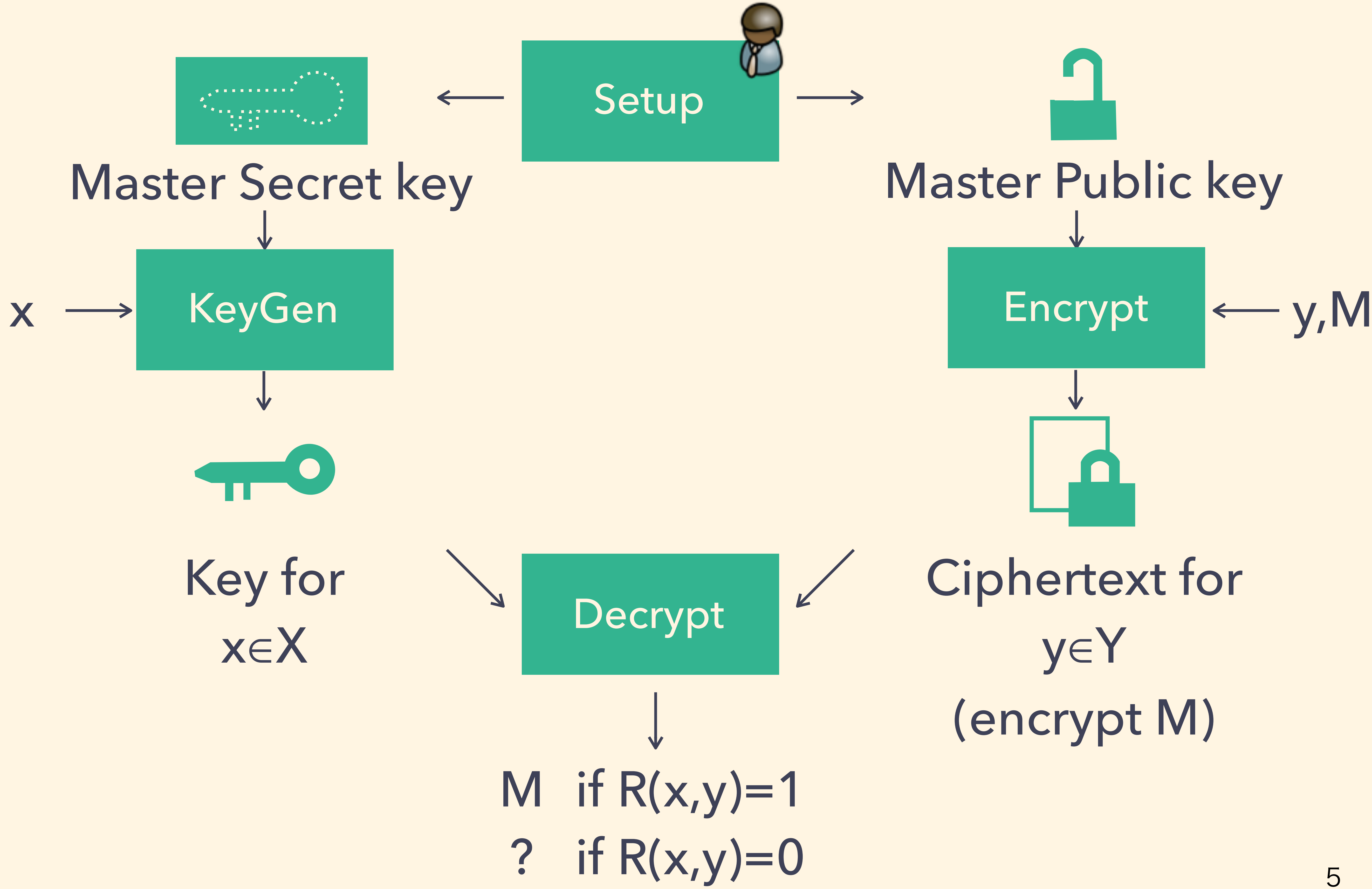
Key for
x∈X

Decrypt

Ciphertext for
y∈Y
(encrypt M)

M if R(x,y)=1
? if R(x,y)=0

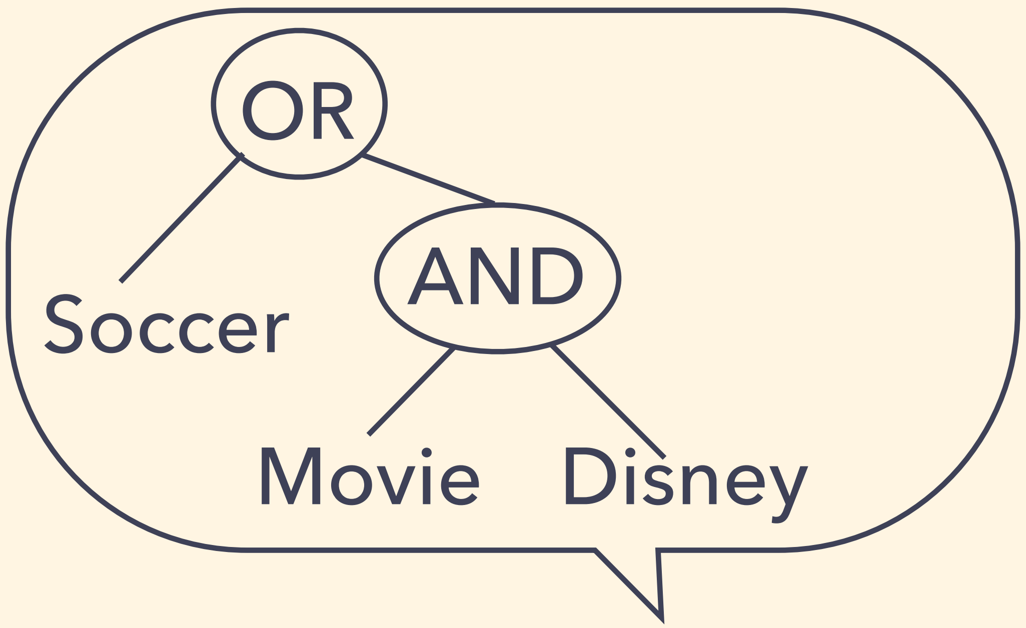
More Complete Picture of ABE



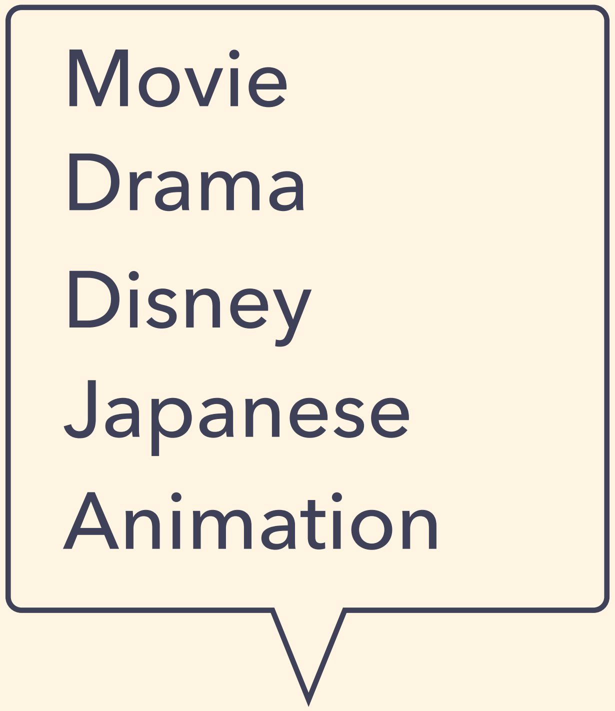
Example of Predicates

1. Key-Policy ABE for Boolean Formulae [GPSW06]

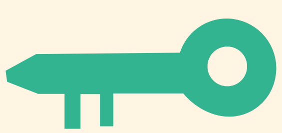
- suitable for content-based access control.

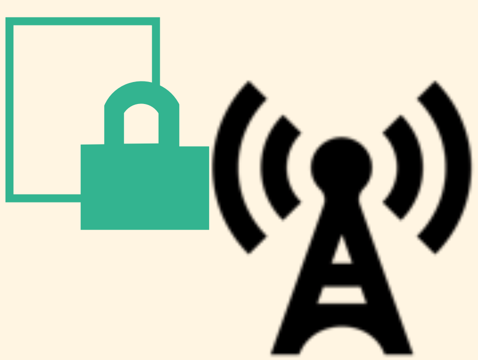


policy x



attribute set y

associated to 

associated to 

- R(x,y)=1 iff y satisfies x.

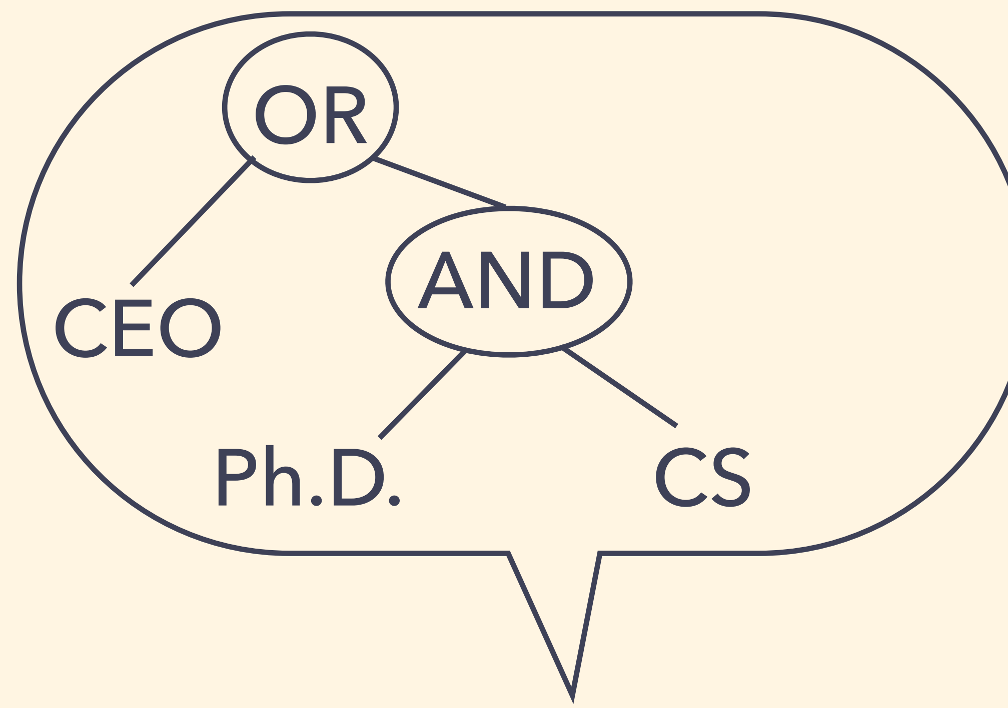
Example of Predicates

2. Ciphertext-Policy ABE for Boolean Formulae [BSW07,W11]

- suitable for person-based access control.

Ph.D.
CS
Thai
Asian

attribute set x



policy y

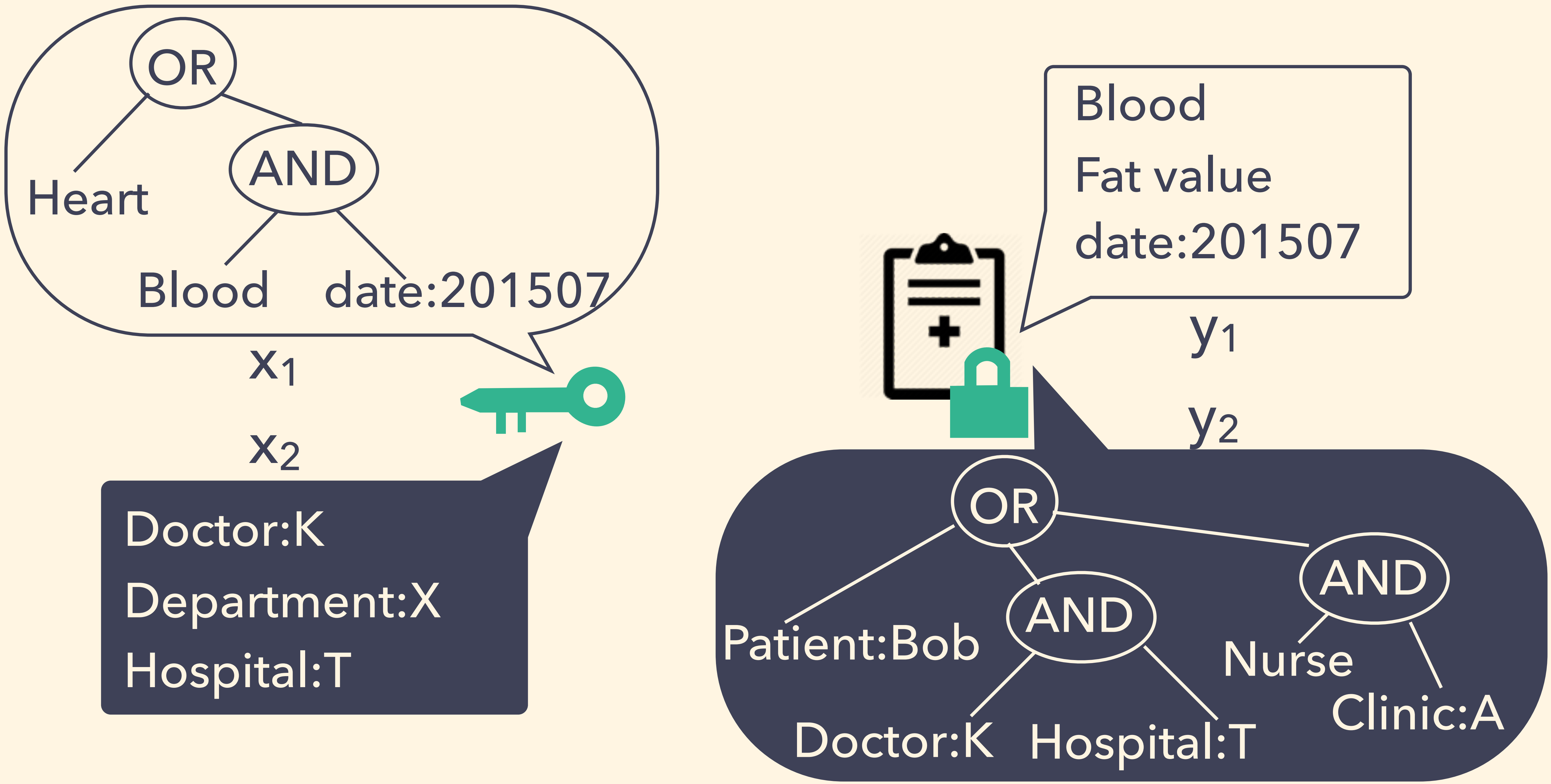
associated to

associated to

- R(x,y)=1 iff x satisfies y.

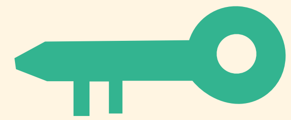
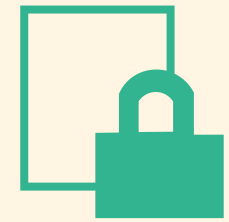
Example of Predicates

3. Dual-Policy ABE for Boolean Formulae [AI09]

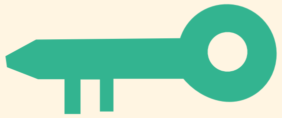


- $R(x,y)=1$ iff y_1 satisfies x_1 *AND* x_2 satisfies y_2.

More Examples of Predicates (1/2)

What Predicate			$R(x, y) = 1$ iff
Identity Based (IBE) [S84, BB04,..]	$x \in \{0,1\}^n$	$y \in \{0,1\}^n$	$x = y$
Inner Product (IPE) [KSW08]	$x \in \mathbb{Z}_p^n$	$y \in \mathbb{Z}_p^n$	$\langle x, y \rangle = 0$
Doubly Spatial (DSE) [H11]	x (affine spaces in $\mathbb{Z}_p^n$)	y	$x \cap y \neq \emptyset$

More Examples of Predicates (2/2)

What Predicate			$R(x, y) = 1$ iff
Span Program [GPSW06, . . .] Finite Automata [W12,A14] Branching Program [GVW13,IW14] Circuits [GGHSW13,GVW13]	$f(\cdot)$ f in that class	y	$f(y) = 1$

Is there a generic way to design ABE for arbitrary predicate R ?

Yes, using recent generic frameworks

[A. Eurocrypt 14], [Wee TCC14]

"Pair encoding" for R $\Rightarrow$ Fully secure ABE for R

+ Subgroup Decision

- Advantage of pair encoding: security is much easier!
  - Perfect [A14,W14]: Info-theoretic argument.
  - Computational [A14]: Similar to selective security.
- But yield ABEs in **composite-order groups**.

Motivation for Prime-order Groups

- Better efficiency than composite-order groups. [G13]
  - Element size: 256 bits vs 3072 bits
  - Bilinear pairing: 254 times faster

Recent Prime-order Frameworks

- [Chen,Gay,Wee EC15], [Agrawal, Chase TCC16]
    - extending [W14,A14].
    - but only for perfect encoding

- **This work**: both perfect & computational encoding

Computational enc covers many more

Computational encoding

- boolean formula [A14,AY15,AHY15]
  - KP, CP, DP
  - fully unbounded
  - short-key or short-ciphertext
- boolean formula over doubly-spatial
  - KP, CP, DP [A14,AY15]
- finite automata (regular language)
  - KP, CP, DP [W12,A14,AY15]

Perfect encoding

- IBE, IPE, Spatial
- boolean formula with some bounds [LOSTW10,W14, A14,...]

Our Main Theorem

Pair encoding for R $\Rightarrow$ **Fully secure ABE for R (Prime-order)**

+ Matrix DH [EHK+13]

Security of pair encoding: same as [A14] ☺

Syntax: **more restricted, but all current encodings satisfy!**

Pair encoding for R $\overset{[A14]}{\Rightarrow}$ **Fully secure ABE for R (Composite-order)**

+ Subgroup Decision

Instantiations: Apply to Existing Encodings

Computational encoding

The first fully-secure & prime-order schemes

- boolean formula [A14,AY15,AHY15]
  - KP, CP, DP
  - fully unbounded
  - short-key or short-ciphertext
- boolean formula over doubly-spatial
  - KP, CP, DP [A14,AY15]
- finite automata (regular language)
  - KP, CP, DP [W12,A14,AY15]
- branching program
  - KP, CP, DP
  - unbounded [new]
  - short-key or short-ciphertext [new]

Perfect encoding

- IBE, IPE, Spatial
- boolean formula with some bounds [LOSTW10,W14, A14,...]

Table 2: Prime-order ABE schemes, positioned by properties

Predicate	Properties		Unbounded		KP	CP	DP
	Security	Universe	Input	Multi-use			
ABE-PDS	full	-	-	-	**New$_1$**	**New$_2$**	**New$_3$**
Unbounded ABE-MSP	selective	large	yes	yes	RW13 [57]	RW13 [57]	sub
	full	small	yes	yes	sub	LW12 [47]	sub
	full	large	yes	no	OT12 [54]	OT12 [54]	sub
	full	large	yes	yes	**New$_4$**	**New$_5$**	**New$_6$**
Short-Cipher ABE-MSP	selective	large	no	yes	ALP11 [8]	sub	sub
	semi	large	no	yes	CW14, T14 [19,60]	AC16 [3]	sub
	full	large	no	yes	**New$_7$**	AHY15 [5]*	**Newer$_{28}$**
Short-Key ABE-MSP	selective	large	no	yes	BGG+14 [12]†	sub	sub
	full	large	no	yes	AHY15 [5]*	**New$_8$**	**Newer$_{29}$**
(Bounded) ABE-MSP	selective	large	no	yes	GPSW06 [34]	W11 [61]	AI09 [6]
	full	small	no	no	CGW15 [17], **New$'_9$**	CGW15 [17], **New$'_{10}$**	**New$_{11}$**
	full	large	no	no	OT10 [52], **New$'_{12}$**	OT10 [52], **New$'_{13}$**	**New$_{14}$**
ABE-RL	selective	small	-	-	W12 [63]	sub	sub
	full	large	-	-	**New$_{15}$**	**New$_{16}$**	**New$_{17}$**
Unbounded ABE-BP	full	-	yes	yes	**New$_{18}$**	**New$_{19}$**	**New$_{20}$**
Short-Cipher ABE-BP	full	-	no	yes	**New$_{21}$**	**Newer$_{27}$**	**Newer$_{30}$**
Short-Key ABE-BP	selective	-	no	yes	GV15 [33]†	sub	sub
	full	-	no	yes	**Newer$_{26}$**	**New$_{22}$**	**Newer$_{31}$**
(Bounded) ABE-BP	selective	-	no	yes	GVW13 [32]†	sub	sub
	full	-	no	no	CGW15 [17], **New$'_{23}$**	CGW15 [17], **New$'_{24}$**	**New$_{25}$**

2 Scheme

Bilinear Maps

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$$

$$\text{PrimeG}(\lambda) \to (e, p, g_1, g_2)$$

$\mathbb{G}_1, \mathbb{G}_2$: groups of prime order p

generators $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$

$$\text{CompositeG}(\lambda) \to (e, N, g_1, \hat{g}_1, g_2, \hat{g}_2)$$

$\mathbb{G}_1, \mathbb{G}_2$: groups of composite order $N = pq$

$g_1 \in \mathbb{G}_{1,p},\ \hat{g}_1 \in \mathbb{G}_{1,q},\ g_2 \in \mathbb{G}_{2,p},\ \hat{g}_2 \in \mathbb{G}_{2,q}$

Pair Encoding Scheme (PES) [A14]

Syntax: $\mathsf{Param}(\kappa) \to n$

$\mathsf{Enc1}(x, N) \to \boldsymbol{k}_x(\alpha, \boldsymbol{r}, \boldsymbol{h})$ and m_1, m_2

$\mathsf{Enc2}(y, N) \to \boldsymbol{c}_y(\boldsymbol{s}, \boldsymbol{h})$ and w_1, w_2

$\mathsf{Pair}(x, y, N) \to \boldsymbol{E} \in \mathbb{Z}_N^{m_1 \times w_1}$

where $\boldsymbol{k}_x \in \mathbb{Z}_N[\alpha, \boldsymbol{r}, \boldsymbol{h}]^{m_1}$ and $\boldsymbol{c}_y \in \mathbb{Z}_N[\boldsymbol{s}, \boldsymbol{h}]^{w_1}$ have variables:

$$\alpha, \boldsymbol{h} = (h_1, \ldots, h_n), \boldsymbol{r} = (r_1, \ldots, r_{m_2}), \boldsymbol{s} = (s_0, \ldots, s_{w_2})$$

and only monomials $\alpha,\ r_i,\ h_k r_i,\ s_j,\ h_k s_j$.

Ensure linearity

Pair Encoding Scheme (PES) [A14]

Syntax: $\mathsf{Param}(\kappa) \to n$

$\mathsf{Enc1}(x, N) \to \boldsymbol{k}_x(\alpha, \boldsymbol{r}, \boldsymbol{h})$ and m_1, m_2

$\mathsf{Enc2}(y, N) \to \boldsymbol{c}_y(\boldsymbol{s}, \boldsymbol{h})$ and w_1, w_2

$\mathsf{Pair}(x, y, N) \to \boldsymbol{E} \in \mathbb{Z}_N^{m_1 \times w_1}$

where $\boldsymbol{k}_x \in \mathbb{Z}_N[\alpha, \boldsymbol{r}, \boldsymbol{h}]^{m_1}$ and $\boldsymbol{c}_y \in \mathbb{Z}_N[\boldsymbol{s}, \boldsymbol{h}]^{w_1}$ have variables:

$$\alpha, \boldsymbol{h} = (h_1, \ldots, h_n), \boldsymbol{r} = (r_1, \ldots, r_{m_2}), \boldsymbol{s} = (s_0, \ldots, s_{w_2})$$

and only monomials $\alpha,\ r_i,\ h_k r_i,\ s_j,\ h_k s_j$.

Correctness: $R(x, y) = 1 \quad \Rightarrow \quad \boldsymbol{k}_x \boldsymbol{E} \boldsymbol{c}_y^\top = \alpha s_0$

Fully Secure ABE from PES [A14, simplified]

$$\begin{aligned}\mathsf{Setup}(\lambda,\kappa):\ & \mathsf{CompositeG}(\lambda) \to (e, N, g_1, \hat{g}_1, g_2, \hat{g}_2),\\ & \mathsf{PES.Param}(\kappa) \to n, \quad \alpha \xleftarrow{\$} \mathbb{Z}_N, \quad \boldsymbol{h} \xleftarrow{\$} \mathbb{Z}_N^n,\\ & \mathsf{PK} = \left(g_1,\, g_1^{\boldsymbol{h}},\, e(g_1, g_2)^{\alpha}\right)\\ & \mathsf{MSK} = \left(g_2,\, g_2^{\boldsymbol{h}},\, g_2^{\alpha}\right)\end{aligned}$$

Fully Secure ABE from PES [A14, simplified]

$$\mathsf{Setup}(\lambda,\kappa):\ \mathsf{CompositeG}(\lambda)\to(e,N,g_1,\hat{g}_1,g_2,\hat{g}_2),$$

$$\mathsf{PES.Param}(\kappa)\to n,\quad \alpha\xleftarrow{\$}\mathbb{Z}_N,\quad \boldsymbol{h}\xleftarrow{\$}\mathbb{Z}_N^n,$$

$$\mathsf{PK}=\left(g_1,\,g_1^{\boldsymbol{h}},\,e(g_1,g_2)^{\alpha}\right)$$

$$\mathsf{MSK}=\left(g_2,\,g_2^{\boldsymbol{h}},\,g_2^{\alpha}\right)$$

$$\mathsf{Encrypt}(\mathsf{PK},y,M):\ \mathsf{PES.Enc2}(y,N)\to(\boldsymbol{c}_y,w_1,w_2),\ \ \boldsymbol{s}\xleftarrow{\$}\mathbb{Z}_N^{w_2},$$

$$\mathsf{CT}=\left(g_1^{\boldsymbol{c}_y(\boldsymbol{s},\boldsymbol{h})},\,e(g_1,g_2)^{\alpha s_0}\cdot M\right)$$

Fully Secure ABE from PES [A14, simplified]

$$\mathsf{Setup}(\lambda,\kappa):\ \mathsf{CompositeG}(\lambda) \to (e, N, g_1, \hat{g}_1, g_2, \hat{g}_2),$$

$$\mathsf{PES.Param}(\kappa) \to n, \quad \alpha \xleftarrow{\$} \mathbb{Z}_N, \quad \boldsymbol{h} \xleftarrow{\$} \mathbb{Z}_N^n,$$

$$\mathsf{PK} = \left(g_1,\ g_1^{\boldsymbol{h}},\ e(g_1,g_2)^{\alpha}\right)$$

$$\mathsf{MSK} = \left(g_2,\ g_2^{\boldsymbol{h}},\ g_2^{\alpha}\right)$$

$$\mathsf{Encrypt}(\mathsf{PK}, y, M):\ \mathsf{PES.Enc2}(y, N) \to (\boldsymbol{c}_y, w_1, w_2), \quad \boldsymbol{s} \xleftarrow{\$} \mathbb{Z}_N^{w_2},$$

$$\mathsf{CT} = \left(g_1^{\boldsymbol{c}_y(\boldsymbol{s},\boldsymbol{h})},\ e(g_1,g_2)^{\alpha s_0}\cdot M\right)$$

$$\mathsf{KeyGen}(\mathsf{MSK}, x):\ \mathsf{PES.Enc1}(x, N) \to (\boldsymbol{k}_x, m_1, m_2), \quad \boldsymbol{r} \xleftarrow{\$} \mathbb{Z}_N^{m_2},$$

$$\mathsf{SK} = g_2^{\boldsymbol{k}_x(\alpha,\boldsymbol{r},\boldsymbol{h})}$$

Fully Secure ABE from PES [A14, simplified]

$$\mathsf{CT} = \left(g_1^{\boldsymbol{c}_y(\boldsymbol{s},\boldsymbol{h})},\ e(g_1,g_2)^{\alpha s_0} \cdot M\right)$$

$$\mathsf{SK} = g_2^{\boldsymbol{k}_x(\alpha,\boldsymbol{r},\boldsymbol{h})}$$

$$\mathsf{Decrypt}(\mathsf{CT}_y, \mathsf{SK}_x):\ \ \mathsf{PES.Pair}(x,y,N) \to \boldsymbol{E},$$

$$\boldsymbol{e}\left(g_1^{\boldsymbol{E}\boldsymbol{c}_y^\top},\ g_2^{\boldsymbol{k}_x^\top}\right) = e(g_1,g_2)^{\boldsymbol{k}_x\boldsymbol{E}\boldsymbol{c}_y^\top} = e(g_1,g_2)^{\alpha s_0}$$

$$\text{where} \quad \boldsymbol{e}(g_1^{\boldsymbol{M}_1}, g_2^{\boldsymbol{M}_2}) := e(g_1,g_2)^{\boldsymbol{M}_2^\top \boldsymbol{M}_1}$$

Fully Secure ABE from PES [A14, simplified]

$$\text{PK} = \left(g_1, g_1^{\boldsymbol{h}}, e(g_1, g_2)^{\alpha}\right)$$

$$\text{MSK} = \left(g_2, g_2^{\boldsymbol{h}}, g_2^{\alpha}\right)$$

$$\text{CT} = \left(g_1^{\boldsymbol{c}_y(\boldsymbol{s},\boldsymbol{h})}, e(g_1, g_2)^{\alpha s_0} \cdot M\right)$$

$$\text{SK} = g_2^{\boldsymbol{k}_x(\alpha,\boldsymbol{r},\boldsymbol{h})}$$

Example: IBE [BB04,LW10]

(h_1, h_2)

$$\mathrm{PK} = \left(g_1,\, g_1^{\boldsymbol{h}},\, e(g_1,g_2)^{\alpha}\right)$$

$$\mathrm{MSK} = \left(g_2,\, g_2^{\boldsymbol{h}},\, g_2^{\alpha}\right)$$

$(s_0(h_1 + y h_2),\ s_0)$

$$\mathrm{CT} = \left(g_1^{\boldsymbol{c}_y(\boldsymbol{s},\boldsymbol{h})},\, e(g_1,g_2)^{\alpha s_0} \cdot M\right)$$

$$\mathrm{SK} = g_2^{\boldsymbol{k}_x(\alpha,\boldsymbol{r},\boldsymbol{h})}$$

$(\alpha + r_1(h_1 + x h_2),\ r_1)$

If $x = y$

$$\left(\alpha + r_1(h_1 + x h_2),\ r_1\right) \underset{\boldsymbol{E}}{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}} \begin{pmatrix} s_0(h_1 y + h_2) \\ s_0 \end{pmatrix} = \alpha s_0$$

Towards Prime-order Setting

Substitute scalar by vector/matrix as in [Chen, Wee C13].

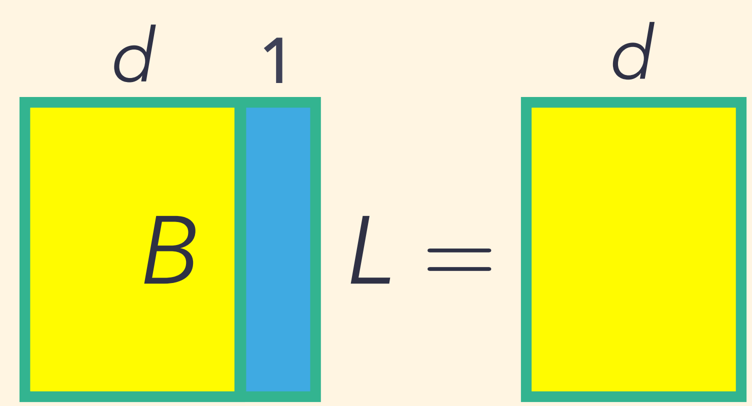
$$\alpha \mapsto \boldsymbol{\alpha} \in \mathbb{Z}_p^{d+1} \qquad h_k \mapsto \boldsymbol{H}_k \in \mathbb{Z}_p^{(d+1)\times(d+1)}$$

$$s_j \mapsto \boldsymbol{s}_j \in \mathbb{Z}_p^{d} \qquad r_i \mapsto \boldsymbol{r}_i \in \mathbb{Z}_p^{d}$$

Generators: pick $\boldsymbol{B}, \boldsymbol{Z} \in \mathbb{Z}_p^{(d+1)\times(d+1)}$ with a distribution $\mathcal{S}_d$,

$$g_1 \mapsto g_1^{\boldsymbol{BL}} \in \mathbb{G}_1^{(d+1)\times d} \qquad g_2 \mapsto g_2^{\boldsymbol{ZL}} \in \mathbb{G}_2^{(d+1)\times d}$$

where $\boldsymbol{L} := \underbrace{\begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ \hline & 0 & \end{bmatrix}}_{d \text{ columns}} \; d+1$.



(left projection)

Towards Prime-order Setting

$$s_j \mapsto \boldsymbol{s}_j \in \mathbb{Z}_p^d \qquad h_k \mapsto \boldsymbol{H}_k \in \mathbb{Z}_p^{(d+1)\times(d+1)}$$

$$g_1 \mapsto g_1^{\boldsymbol{BL}} \in \mathbb{G}_1^{(d+1)\times d}$$

Exponentiations:

$$g_1^{h_k} \mapsto g_1^{\boldsymbol{H}_k\boldsymbol{BL}} \in \mathbb{G}_1^{(d+1)\times d}$$

$$g_1^{s_j} \mapsto g_1^{\boldsymbol{BL}\boldsymbol{s}_j} \in \mathbb{G}_1^{(d+1)\times 1}$$

$$g_1^{h_k s_j} \mapsto g_1^{\boldsymbol{H}_k\boldsymbol{BL}\boldsymbol{s}_j} \in \mathbb{G}_1^{(d+1)\times 1}$$

(tweaked from [CW13], which is not directly applicable.)

Subgroup-Decision | Matrix-DH [EHK+13]

Composite-order groups

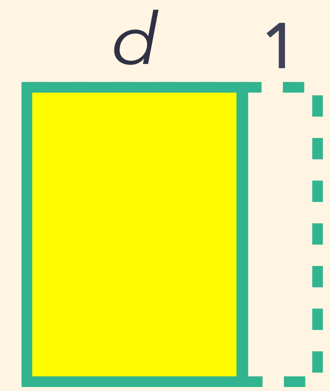
$$g_1^{s_j} \approx g_1^{s_j} \hat{g}_1^{\hat{s}_j}$$

$\mathbb{G}_{1,p_1}$ $\quad$ $\mathbb{G}_{1,p} \times \mathbb{G}_{1,q}$

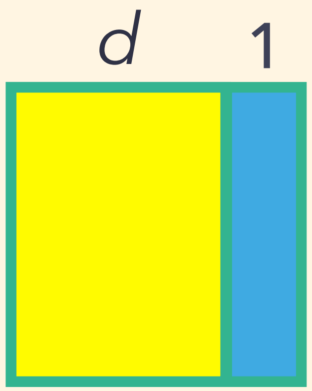
subgroup $\quad$ whole group

Prime-order groups

$$g_1^{\boldsymbol{BLs}_j} \approx g_1^{\boldsymbol{BLs}_j} g_1^{\boldsymbol{BJ}\hat{s}_j}$$



subspace



whole space

($J =$ right projection)

- d-DLIN is an instance.

Our Prime-order ABE from PES

$$\mathsf{Setup}(\lambda,\kappa):\ \ \mathsf{PrimeG}(\lambda) \to (e,p,g_1,g_2),\quad \text{pick } \boldsymbol{B},\boldsymbol{Z} \xleftarrow{\$} \mathcal{S}_d,$$

$$\boldsymbol{\alpha} \xleftarrow{\$} \mathbb{Z}_p^{d+1}, \qquad \boldsymbol{H}_i \xleftarrow{\$} \mathbb{Z}_p^{(d+1)\times(d+1)},$$

$$\mathsf{PK} = \left(g_1^{\boldsymbol{BL}},\ g_1^{\boldsymbol{H}_1\boldsymbol{BL}},\ldots,g_1^{\boldsymbol{H}_n\boldsymbol{BL}},\ e(g_1,g_2)^{\boldsymbol{\alpha}^\top\boldsymbol{BL}}\right)$$

$$\mathsf{MSK} = \left(g_2^{\boldsymbol{ZL}},\ g_2^{\boldsymbol{H}_1^\top\boldsymbol{ZL}},\ldots,g_2^{\boldsymbol{H}_n^\top\boldsymbol{ZL}},\ g_2^{\boldsymbol{\alpha}}\right)$$

emulate g_1, g_1^{h}

Our Prime-order ABE from PES

$$\mathrm{PK} = \left(g_1^{\boldsymbol{BL}}, g_1^{\boldsymbol{H}_1\boldsymbol{BL}}, \ldots, g_1^{\boldsymbol{H}_n\boldsymbol{BL}}, e(g_1, g_2)^{\boldsymbol{\alpha}^\top \boldsymbol{BL}}\right)$$

$$\mathrm{MSK} = \left(g_2^{\boldsymbol{ZL}}, g_2^{\boldsymbol{H}_1^\top\boldsymbol{ZL}}, \ldots, g_2^{\boldsymbol{H}_n^\top\boldsymbol{ZL}}, g_2^{\boldsymbol{\alpha}}\right)$$

$$\mathsf{Encrypt}(\mathrm{PK}, y, M): \ \boldsymbol{S} \xleftarrow{\$} \mathbb{Z}_p^{d\times(w_2+1)},$$

$$\mathrm{CT}_y = \left(g_1^{\boldsymbol{c}_y\left(\boldsymbol{BLS}, \mathbb{H}\right)}, e(g_1, g_2)^{\boldsymbol{\alpha}^\top \boldsymbol{BLs}_0} \cdot M\right)$$

$$\mathsf{KeyGen}(\mathrm{MSK}, x): \quad \boldsymbol{R} \xleftarrow{\$} \mathbb{Z}_p^{d\times m_2},$$

$$\mathrm{SK}_x = g_2^{\boldsymbol{k}_x\left(\boldsymbol{\alpha}, \boldsymbol{ZLR}, \mathbb{H}\right)}$$

Our Prime-order ABE from PES

$$\mathrm{PK} = \left(g_1^{\boldsymbol{BL}},\ g_1^{\boldsymbol{H}_1\boldsymbol{BL}}, \ldots, g_1^{\boldsymbol{H}_n\boldsymbol{BL}},\ e(g_1, g_2)^{\boldsymbol{\alpha}^\top \boldsymbol{BL}}\right)$$

$$\mathrm{MSK} = \left(g_2^{\boldsymbol{ZL}},\ g_2^{\boldsymbol{H}_1^\top \boldsymbol{ZL}}, \ldots, g_2^{\boldsymbol{H}_n^\top \boldsymbol{ZL}},\ g_2^{\boldsymbol{\alpha}}\right)$$

$$\mathrm{Encrypt}(\mathrm{PK}, y, M):\ \boldsymbol{S} \xleftarrow{\$} \mathbb{Z}_p^{d\times(w_2+1)}$$

$$\mathrm{CT}_y = \left(g_1^{\boldsymbol{c}_y\left(\boldsymbol{BLS},\, \mathbb{H}\right)}\right.$$

$$g_1^{\boldsymbol{c}_y(\boldsymbol{s},\boldsymbol{h})} \mapsto g_1^{\boldsymbol{c}_y\left(\boldsymbol{BLS},\, \mathbb{H}\right)}$$

$$g_1^{s_j} \mapsto g_1^{\boldsymbol{BLs}_j}$$

$$g_1^{h_k s_j} \mapsto g_1^{\boldsymbol{H}_k\boldsymbol{BLs}_j}$$

$$\mathrm{KeyGen}(\mathrm{MSK}, x):\quad \boldsymbol{R} \xleftarrow{\$} \mathbb{Z}_p^{d\times m_2},$$

$$\mathrm{SK}_x = g_2^{\boldsymbol{k}_x\left(\boldsymbol{\alpha},\, \boldsymbol{ZLR},\, \mathbb{H}\right)}$$

$$\mathbb{H} = (\boldsymbol{H}_1, \ldots, \boldsymbol{H}_n)$$

Our Prime-order ABE from PES

$$\mathrm{PK} = \left(g_1^{\boldsymbol{BL}}, g_1^{\boldsymbol{H}_1\boldsymbol{BL}}, \ldots, g_1^{\boldsymbol{H}_n\boldsymbol{BL}}, e(g_1, g_2)^{\boldsymbol{\alpha}^\top \boldsymbol{BL}}\right)$$

$$\mathrm{MSK} = \left(g_2^{\boldsymbol{ZL}}, g_2^{\boldsymbol{H}_1^\top \boldsymbol{ZL}}, \ldots, g_2^{\boldsymbol{H}_n^\top \boldsymbol{ZL}}, g_2^{\boldsymbol{\alpha}}\right)$$

$\mathrm{Encrypt}(\mathrm{PK}, y, M): \ \boldsymbol{S} \xleftarrow{\$} \mathbb{Z}_p^{d \times (w_2+1)},$

$$\mathrm{CT}_y = \left(g_1^{\boldsymbol{c}_y\left(\boldsymbol{BLS}, \mathbb{H}\right)}, \right.$$

$\mathrm{KeyGen}(\mathrm{MSK}, x): \quad \boldsymbol{R} \xleftarrow{\$} \mathbb{Z}_p^{d \times n}$

$$\mathrm{SK}_x = g_2^{\boldsymbol{k}_x\left(\boldsymbol{\alpha}, \boldsymbol{ZLR}, \mathbb{H}\right)}$$

$$g_2^{\boldsymbol{k}_x(\alpha, \boldsymbol{r}, \boldsymbol{h})} \mapsto g_2^{\boldsymbol{k}_x\left(\boldsymbol{\alpha}, \boldsymbol{ZLR}, \mathbb{H}\right)}$$

$$g_2^{r_i} \mapsto g_2^{\boldsymbol{ZLr}_i}$$

$$g_2^{h_k r_i} \mapsto g_2^{\boldsymbol{H}_k^\top \boldsymbol{ZLr}_i}$$

Our Prime-order ABE from PES

$$\mathrm{CT}_y = \left(g_1^{\boldsymbol{c}_y\left(\boldsymbol{BLS}, \mathbb{H}\right)}, \, e(g_1, g_2)^{\boldsymbol{\alpha}^\top \boldsymbol{BLs}_0} \cdot M \right)$$

$$\mathrm{SK}_x = g_2^{\boldsymbol{k}_x\left(\boldsymbol{\alpha}, \boldsymbol{ZLR}, \mathbb{H}\right)}$$

$$\mathrm{Decrypt}(\mathrm{CT}_y, \mathrm{SK}_x) : \quad \mathrm{PES.Pair}(x, y, p) \to \boldsymbol{E},$$

$$\prod_{\substack{i \in [1, m_1] \\ j \in [1, w_1]}} \boldsymbol{e}(g_1^{\boldsymbol{c}_y[j]}, g_2^{\boldsymbol{k}_x[i]})^{\boldsymbol{E}_{i,j}} = e(g_1, g_2)^{\boldsymbol{\alpha}^\top \boldsymbol{BLs}_0}$$

Correctness: Use Associativity [CW13]

Correctness of PES implicitly uses

$$s_j \cdot (h_k r_i) = (h_k s_j) \cdot r_i$$

In bilinear map on scalars (as used in [A14]), we have

$$e(g_1^{s_j}, g_2^{h_k r_i}) = e(g_1^{h_k s_j}, g_2^{r_i})$$

In bilinear map on vectors here, we have

$$\mathbf{e}(g_1^{\boldsymbol{a}}, g_2^{\boldsymbol{H}_k^\top \boldsymbol{b}}) = \mathbf{e}(g_1^{\boldsymbol{H}_k \boldsymbol{a}}, g_2^{\boldsymbol{b}})$$

since $\quad e(g_1, g_2)^{(\boldsymbol{b}^\top \boldsymbol{H}_k)\cdot \boldsymbol{a}} = e(g_1, g_2)^{\boldsymbol{b}^\top \cdot (\boldsymbol{H}_k \boldsymbol{a})}$

and recall $\quad \mathbf{e}(g_1^{\boldsymbol{M}_1}, g_2^{\boldsymbol{M}_2}) := e(g_1, g_2)^{\boldsymbol{M}_2^\top \boldsymbol{M}_1}$

What About Commutativity?

Correctness of PES also implicitly (possibly) uses

$$(h_\ell s_j)\cdot(h_k r_i) = (h_k s_j)\cdot(h_\ell r_i)$$

In bilinear map on scalars (as used in [A14]), we have

$$e(g_1^{h_\ell s_j}, g_2^{h_k r_i}) = e(g_1^{h_k s_j}, g_2^{h_\ell r_i})$$

But, in bilinear map on vectors here, we have

$$e(g_1^{\boldsymbol{H}_\ell \boldsymbol{a}}, g_2^{\boldsymbol{H}_k^\top \boldsymbol{b}}) \neq e(g_1^{\boldsymbol{H}_k \boldsymbol{a}}, g_2^{\boldsymbol{H}_\ell^\top \boldsymbol{b}})$$

since $e(g_1, g_2)^{(\boldsymbol{b}^\top \boldsymbol{H}_k)\cdot(\boldsymbol{H}_\ell \boldsymbol{a})} \neq e(g_1, g_2)^{(\boldsymbol{b}^\top \boldsymbol{H}_\ell)\cdot(\boldsymbol{H}_k \boldsymbol{a})}$

What About Commutativity? –No.

Correctness of PES also implicitly (possibly) uses

$$(h_\ell s_j) \cdot (h_k r_i) = (h_k s_j) \cdot (h_\ell r_i)$$

Hence, we simply restrict PES to exclude these.

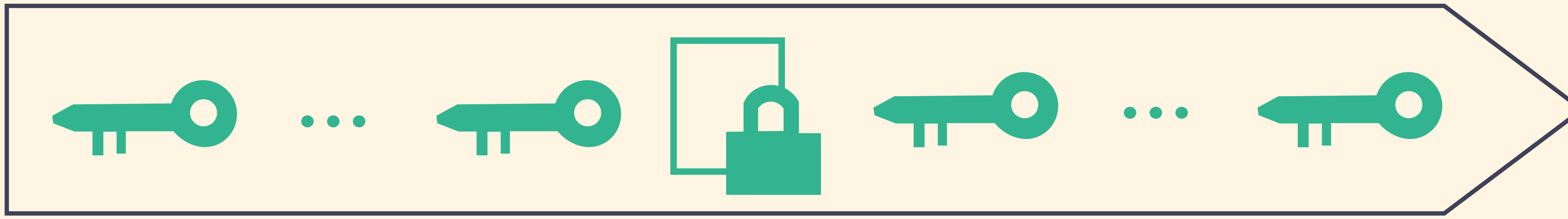
Done by restricting E outputted from Pair.

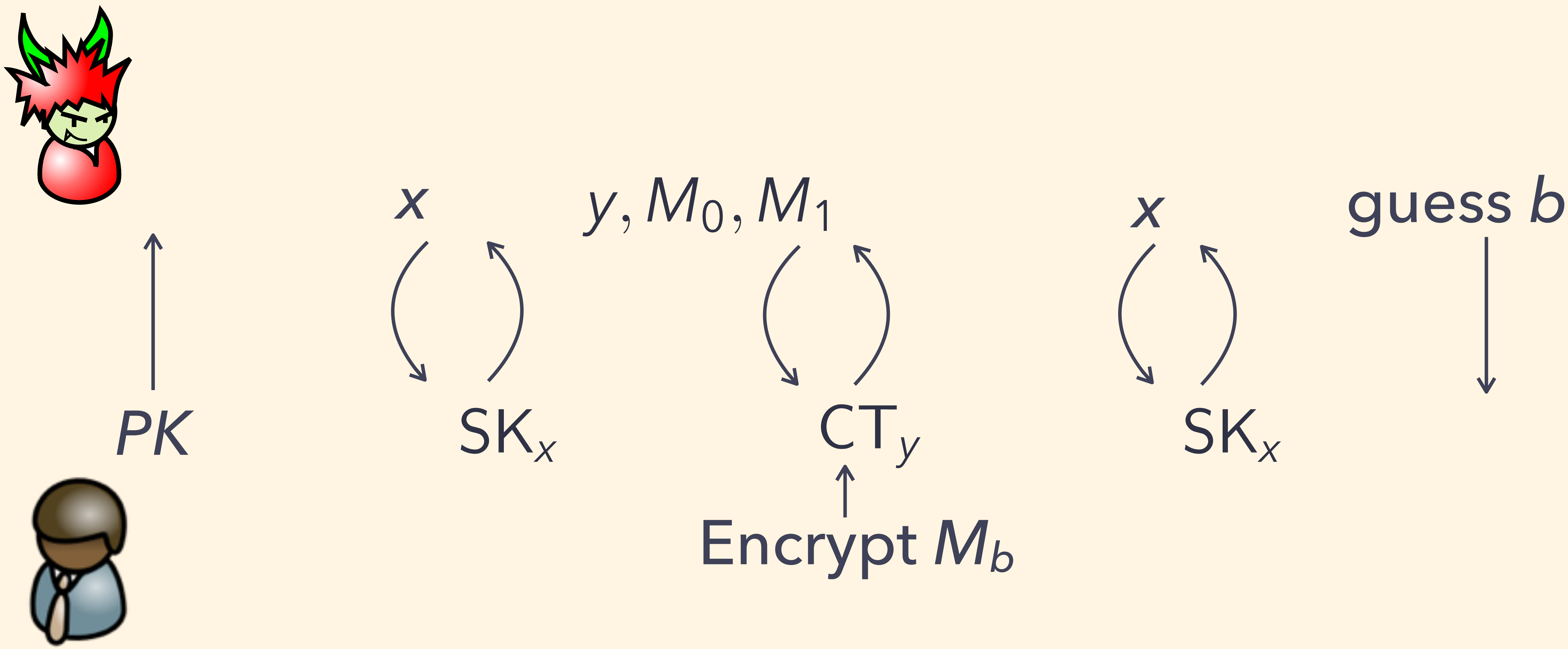
Call this as Rule I.

3 Security Proof

Definition for Full Security

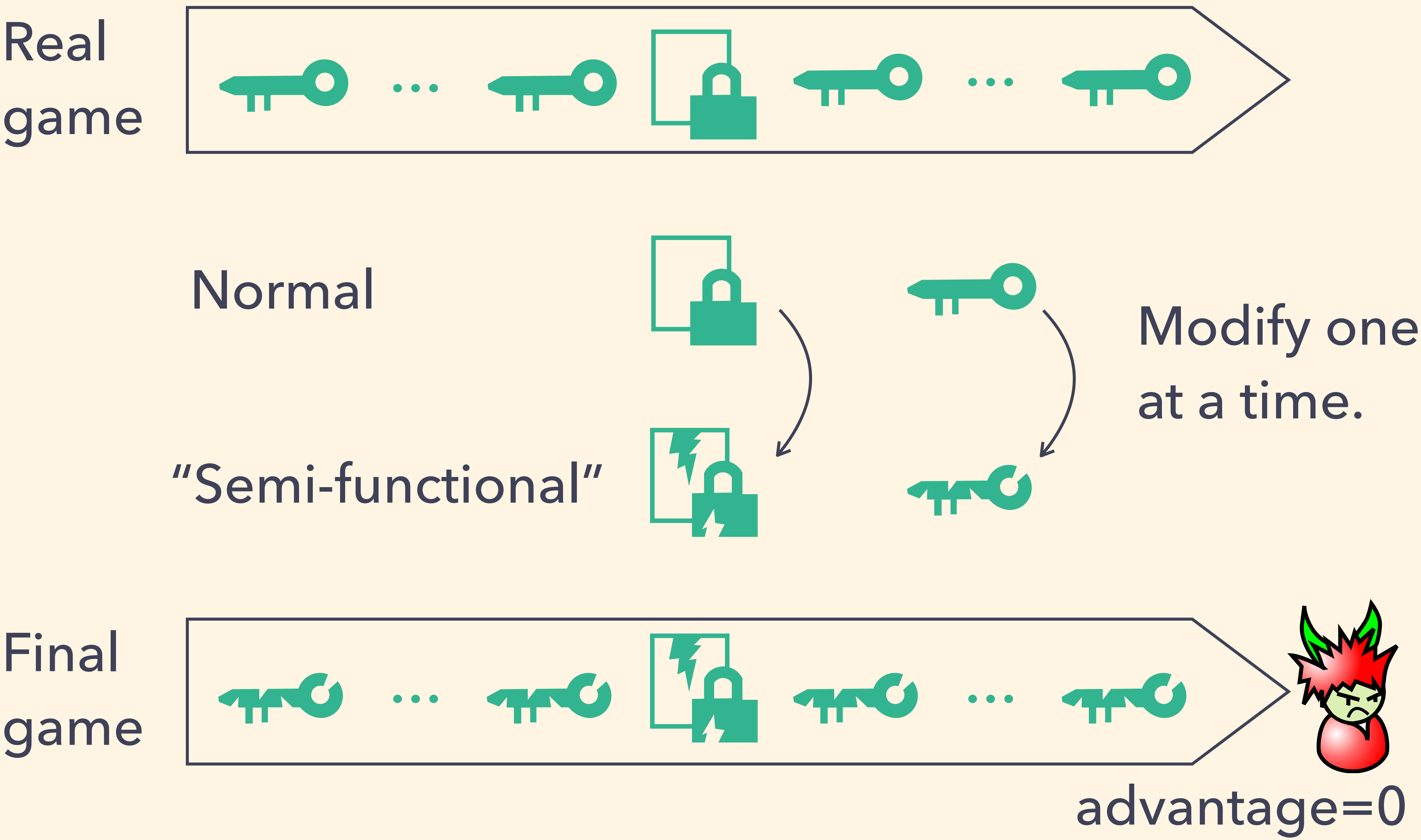
Pictorially in timeline



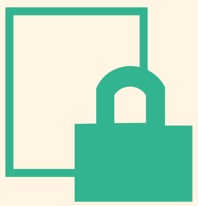


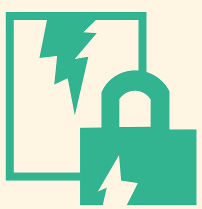
condition: $R(x, y) = 0$

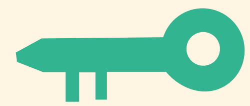
"Dual System" Proof Method [W09]

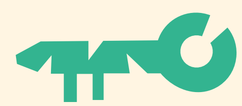


Semi-Functional (SF) Ciphertext/Key in [A14]

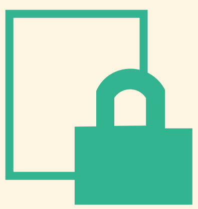
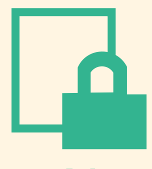
 $= g_1^{\mathbf{c}_y(\mathbf{s},\mathbf{h})}$

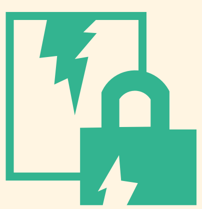
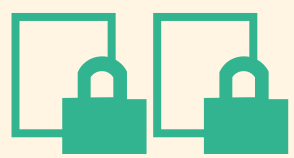
 $= g_1^{\mathbf{c}_y(\mathbf{s},\mathbf{h})}\,\hat{g}_1^{\mathbf{c}_y(\hat{\mathbf{s}},\hat{\mathbf{h}})}$

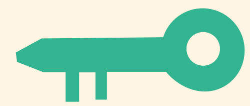
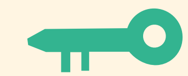
 $= g_2^{\mathbf{k}_x(\alpha,\mathbf{r},\mathbf{h})}$

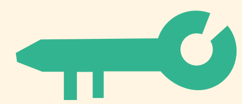
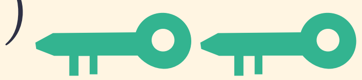
 $= g_2^{\mathbf{k}_x(\alpha,\mathbf{r},\mathbf{h})}\,\hat{g}_2^{\mathbf{k}_x(\hat{\alpha},\mathbf{0},\mathbf{0})}$

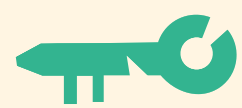
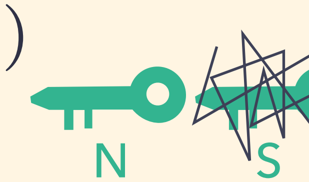
Semi-Functional (SF) Ciphertext/Key in [A14]

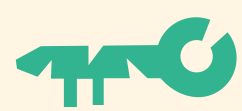
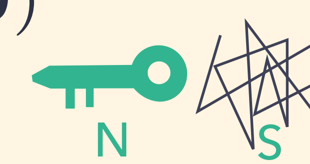

$= g_1^{\boldsymbol{c}_y(\boldsymbol{s},\boldsymbol{h})}$



$= g_1^{\boldsymbol{c}_y(\boldsymbol{s},\boldsymbol{h})}\,\hat{g}_1^{\boldsymbol{c}_y(\hat{\boldsymbol{s}},\hat{\boldsymbol{h}})}$



$= g_2^{\boldsymbol{k}_x(\alpha,\boldsymbol{r},\boldsymbol{h})}$



$= g_2^{\boldsymbol{k}_x(\alpha,\boldsymbol{r},\boldsymbol{h})}\,\hat{g}_2^{\boldsymbol{k}_x(0,\hat{\boldsymbol{r}},\hat{\boldsymbol{h}})}$


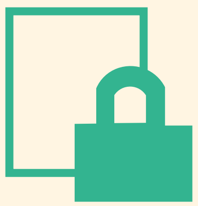

$= g_2^{\boldsymbol{k}_x(\alpha,\boldsymbol{r},\boldsymbol{h})}\,\hat{g}_2^{\boldsymbol{k}_x(\hat{\alpha},\hat{\boldsymbol{r}},\hat{\boldsymbol{h}})}$


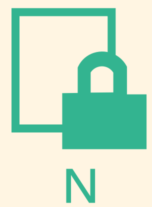

$= g_2^{\boldsymbol{k}_x(\alpha,\boldsymbol{r},\boldsymbol{h})}\,\hat{g}_2^{\boldsymbol{k}_x(\hat{\alpha},\boldsymbol{0},\boldsymbol{0})}$


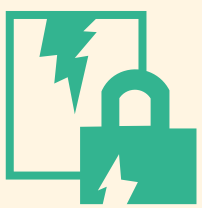
More “concretely” …

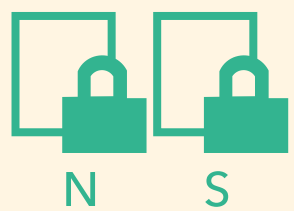

SF
San
KEYCHAIN
Francisco
"YOUR KEY TO THE CITY"

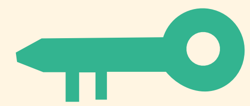
Proof Intuition 1 [A14]

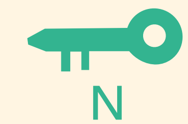
 $= g_1^{c_y(\mathbf{s},\mathbf{h})}$

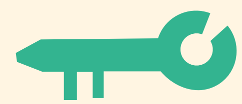


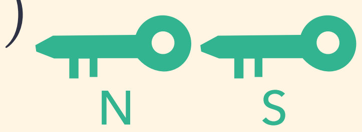
 $= g_1^{c_y(\mathbf{s},\mathbf{h})}\ \hat{g}_1^{c_y(\hat{\mathbf{s}},\hat{\mathbf{h}})}$

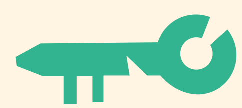


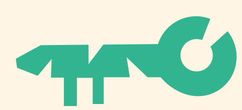
 $= g_2^{\mathbf{k}_x(\alpha,\mathbf{r},\mathbf{h})}$

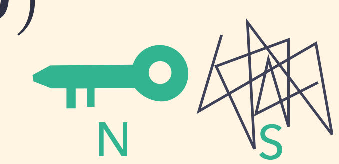


 $= g_2^{\mathbf{k}_x(\alpha,\mathbf{r},\mathbf{h})}\ \hat{g}_2^{\mathbf{k}_x(0,\hat{\mathbf{r}},\hat{\mathbf{h}})}$



 $= g_2^{\mathbf{k}_x(\alpha,\mathbf{r},\mathbf{h})}\ \hat{g}_2^{\mathbf{k}_x(\hat{\alpha},\hat{\mathbf{r}},\hat{\mathbf{h}})}$

 $= g_2^{\mathbf{k}_x(\alpha,\mathbf{r},\mathbf{h})}\ \hat{g}_2^{\mathbf{k}_x(\hat{\alpha},\mathbf{0},\mathbf{0})}$

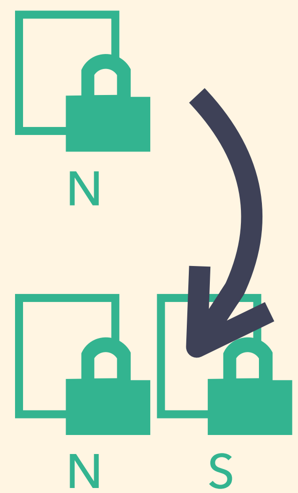


Proof Intuition 1 [A14]

"Copy" from Normal to SF can use Subgroup Decision.

$$= g_1^{\boldsymbol{c}_y(\boldsymbol{s},\boldsymbol{h})}$$

$$= g_1^{\boldsymbol{c}_y(\boldsymbol{s},\boldsymbol{h})}\ \hat{g}_1^{\boldsymbol{c}_y(\hat{\boldsymbol{s}},\hat{\boldsymbol{h}})}$$

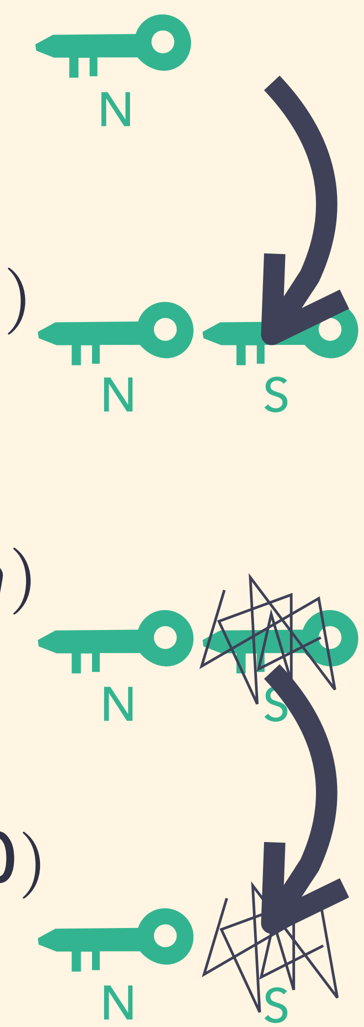


$$= g_2^{\boldsymbol{k}_x(\alpha,\boldsymbol{r},\boldsymbol{h})}$$

$$= g_2^{\boldsymbol{k}_x(\alpha,\boldsymbol{r},\boldsymbol{h})}\ \hat{g}_2^{\boldsymbol{k}_x(0,\hat{\boldsymbol{r}},\hat{\boldsymbol{h}})}$$

$$= g_2^{\boldsymbol{k}_x(\alpha,\boldsymbol{r},\boldsymbol{h})}\ \hat{g}_2^{\boldsymbol{k}_x(\hat{\alpha},\hat{\boldsymbol{r}},\hat{\boldsymbol{h}})}$$

$$= g_2^{\boldsymbol{k}_x(\alpha,\boldsymbol{r},\boldsymbol{h})}\ \hat{g}_2^{\boldsymbol{k}_x(\hat{\alpha},\boldsymbol{0},\boldsymbol{0})}$$

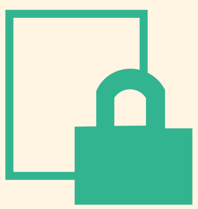


Subgroup Decision

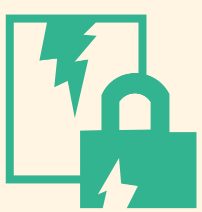
$$g_1^{s_j} \approx g_1^{s_j}\hat{g}_1^{\hat{s}_j}$$

Proof Intuition 2 [A14]

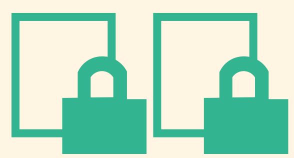
The only remaining hybrid uses the security of PES.

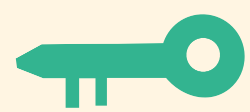


$= g_1^{c_y(\boldsymbol{s},\boldsymbol{h})}$

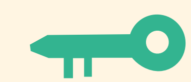


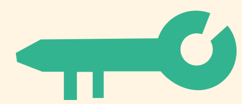
$= g_1^{c_y(\boldsymbol{s},\boldsymbol{h})} \hat{g}_1^{c_y(\hat{\boldsymbol{s}},\hat{\boldsymbol{h}})}$



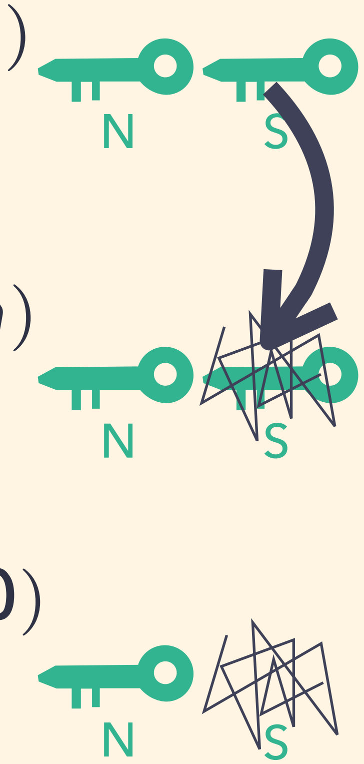


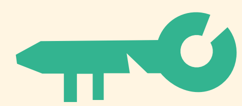
$= g_2^{\boldsymbol{k}_x(\alpha,\boldsymbol{r},\boldsymbol{h})}$



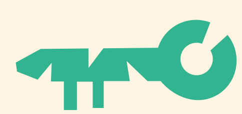


$= g_2^{\boldsymbol{k}_x(\alpha,\boldsymbol{r},\boldsymbol{h})} \hat{g}_2^{\boldsymbol{k}_x(0,\hat{\boldsymbol{r}},\hat{\boldsymbol{h}})}$



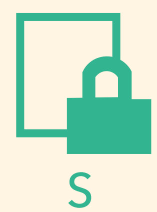


$= g_2^{\boldsymbol{k}_x(\alpha,\boldsymbol{r},\boldsymbol{h})} \hat{g}_2^{\boldsymbol{k}_x(\hat{\alpha},\hat{\boldsymbol{r}},\hat{\boldsymbol{h}})}$



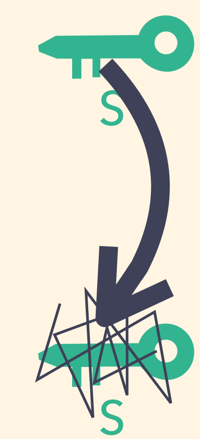
$= g_2^{\boldsymbol{k}_x(\alpha,\boldsymbol{r},\boldsymbol{h})} \hat{g}_2^{\boldsymbol{k}_x(\hat{\alpha},\boldsymbol{0},\boldsymbol{0})}$

$\hat{g}_1^{\boldsymbol{c}_y(\hat{\boldsymbol{s}},\hat{\boldsymbol{h}})}$



$\hat{g}_2^{\boldsymbol{k}_x(0,\hat{\boldsymbol{r}},\hat{\boldsymbol{h}})}$

$\hat{g}_2^{\boldsymbol{k}_x(\hat{\alpha},\hat{\boldsymbol{r}},\hat{\boldsymbol{h}})}$

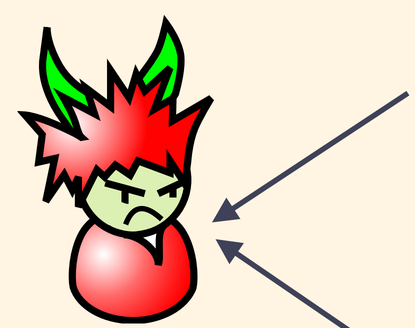


Definition for Security of PES [A14]

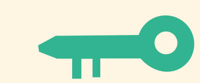
Computational security [A14] **:** For x, y s.t. $R(x, y) = 0$,

Given $\hat{g}_1^{\boldsymbol{c}_y(\hat{\boldsymbol{s}},\hat{\boldsymbol{h}})}$

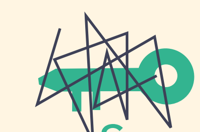
which?



$\hat{g}_2^{\boldsymbol{k}_x(0,\hat{\boldsymbol{r}},\hat{\boldsymbol{h}})}$



$\hat{g}_2^{\boldsymbol{k}_x(\hat{\alpha},\hat{\boldsymbol{r}},\hat{\boldsymbol{h}})}$



(each x, y is queried once by  in any order.)

Perfect security [A14, W14] **:** info-theoretic sense.

Our Scheme: SF Ciphertext/Key

$g_1^{c_y(BLS, \mathbb{H})}$ N

$g_1^{c_y(BLS, \mathbb{H})} \, g_1^{c_y(BJ\hat{S}, \mathbb{H})}$ N S

$g_2^{k_x(\alpha, ZLR, \mathbb{H})}$ N

$g_2^{k_x(\alpha, ZLR, \mathbb{H})} \, g_2^{k_x(0, ZJ\hat{R}, \mathbb{H})}$ N S

$g_2^{k_x(\alpha, ZLR, \mathbb{H})} \, g_2^{k_x(\hat{\alpha}, ZJ\hat{R}, \mathbb{H})}$ N S

$g_2^{k_x(\alpha, ZLR, \mathbb{H})} \, g_2^{k_x(\hat{\alpha}, 0, 0)}$ N S

Our Proof Intuition 1

"Copy" now uses Matrix Diffie-Hellman [EHK+13].

$$g_1^{c_y(BLS, \mathbb{H})}$$

$$g_1^{c_y(BLS, \mathbb{H})} \; g_1^{c_y(BJ\hat{S}, \mathbb{H})}$$

Matrix DH

$$g_1^{BLs_j} \approx g_1^{BLs_j} g_1^{BJ\hat{s}_j}$$

$$g_2^{k_x(\alpha, ZLR, \mathbb{H})}$$

$$g_2^{k_x(\alpha, ZLR, \mathbb{H})} \; g_2^{k_x(0, ZJ\hat{R}, \mathbb{H})}$$

$$g_2^{k_x(\alpha, ZLR, \mathbb{H})} \; g_2^{k_x(\hat{\alpha}, ZJ\hat{R}, \mathbb{H})}$$

$$g_2^{k_x(\alpha, ZLR, \mathbb{H})} \; g_2^{k_x(\hat{\alpha}, 0, 0)}$$

New technique uses random self-reducibility of Mat-DH.

Our Proof Intuition 2

Goal: The remaining hybrid will use the security of PES.

$$g_1^{c_y(BLS,\mathbb{H})}$$

$$g_1^{c_y(BLS,\mathbb{H})}\, g_1^{c_y(BJ\hat{S},\mathbb{H})}$$

$$g_2^{k_x(\alpha, ZLR, \mathbb{H})}$$

$$g_2^{k_x(\alpha, ZLR, \mathbb{H})}\, g_2^{k_x(0, ZJ\hat{R}, \mathbb{H})}$$

$$g_2^{k_x(\alpha, ZLR, \mathbb{H})}\, g_2^{k_x(\hat{\alpha}, ZJ\hat{R}, \mathbb{H})}$$

$$g_2^{k_x(\alpha, ZLR, \mathbb{H})}\, g_2^{k_x(\hat{\alpha}, 0, 0)}$$

Problem: But security of PES was not in "matrix-form".

Need to find a condition for reduction

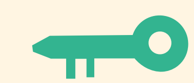
so that the security of PES implies exactly this hybrid.

Given $g_1^{\boldsymbol{c}_y\left(BJ\hat{S},\, \mathbb{H}\right)}$

S

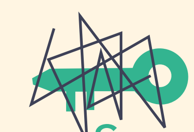
which?

$g_2^{\boldsymbol{k}_x\left(\mathbf{0},\, ZJ\hat{R},\, \mathbb{H}\right)}$



S

$g_2^{\boldsymbol{k}_x\left(\hat{\alpha},\, ZJ\hat{R},\, \mathbb{H}\right)}$



S

Need to find a condition for reduction

Given $\hat{g}_1^{\boldsymbol{c}_y(\hat{\boldsymbol{s}},\hat{\boldsymbol{h}})}$ s

which?

$\hat{g}_2^{\boldsymbol{k}_x(0,\hat{\boldsymbol{r}},\hat{\boldsymbol{h}})}$ s

$\hat{g}_2^{\boldsymbol{k}_x(\hat{\alpha},\hat{\boldsymbol{r}},\hat{\boldsymbol{h}})}$ s

Security of PES

Given $g_1^{\boldsymbol{c}_y\left(\boldsymbol{B}\boldsymbol{J}\hat{\boldsymbol{S}},\,\mathbb{H}\right)}$ s

which?

$g_2^{\boldsymbol{k}_x\left(\boldsymbol{0},\,\boldsymbol{Z}\boldsymbol{J}\hat{\boldsymbol{R}},\,\mathbb{H}\right)}$ s

$g_2^{\boldsymbol{k}_x\left(\hat{\alpha},\,\boldsymbol{Z}\boldsymbol{J}\hat{\boldsymbol{R}},\,\mathbb{H}\right)}$ s

Our hybrid

Need to find a co

Given $\hat{g}_1^{c_y(\hat{s},\hat{h})}$

S

Security of PES

Given $g_1^{c_y\left(BJ\hat{S},\,\mathbb{H}\right)}$

S

Our hybrid

Our conditions:

Can be defined solely on *syntax*.

- *$h_k r_i$ allowed only if r_i is in k_x.*
- *$h_k s_j$ allowed only if s_j is in c_y.*
- *s_0 is in c_y.*

Call these as Rule 2,3,4.

Wrapping Up to Our Theorem

PES for R $\Rightarrow$ **Fully secure ABE for R (Prime-order)**

+ Matrix DH [EHK+13]

- PES syntax is restricted to Rule 1,2,3,4.
- PES security is unchanged from [A14].

Concluding Remarks

- We presented a generic conversion from pair encoding to fully secure ABE in prime-order groups.
- It implies the first fully secure prime-order ABE instantiations for many predicates.
- Omitted here:
  - tighter reduction as in [A14].
  - can use simpler basis [CGW15], instead of [CW13].