Déjà Q: Using Dual Systems to Revisit q-Type Assumptions

Melissa Chase (MSR Redmond)

Sarah Meiklejohn (UC San Diego → University College London)

Pairing-based cryptography: a brief history

Historically, pairings have provided great functionality

Pairing-based cryptography: a brief history

Historically, pairings have provided great functionality

- First IBE instantiation [BF01]

Pairing-based cryptography: a brief history

Historically, pairings have provided great functionality

- First IBE instantiation [BF01]
- Many other breakthroughs have followed [BBS04,GS08,KSW08,LW11,...]

Pairing-based cryptography: a brief history

Historically, pairings have provided great functionality

- First IBE instantiation [BF01]
- Many other breakthroughs have followed [BBS04,GS08,KSW08,LW11,...]

With great functionality, comes great (ir)responsibility!

Pairing-based cryptography: a brief history

Historically, pairings have provided great functionality

- First IBE instantiation [BF01]
- Many other breakthroughs have followed [BBS04,GS08,KSW08,LW11,...]

With great functionality, comes great (ir)responsibility!


First assumption: BDH (given (g^a, g^b, g^c), compute $e(g,g)^{abc}$)

Pairing-based cryptography: a brief history

Historically, pairings have provided great functionality

- First IBE instantiation [BF01]
- Many other breakthroughs have followed [BBS04,GS08,KSW08,LW11,...]

With great functionality, comes great (ir)responsibility!

 First assumption: BDH (given (g^a,g^b,g^c), compute $e(g,g)^{abc}$)

 Later assumptions: Subgroup Hiding [BGN05], Decision Linear, SXDH

Pairing-based cryptography: a brief history

Historically, pairings have provided great functionality

- First IBE instantiation [BF01]
- Many other breakthroughs have followed [BBS04,GS08,KSW08,LW11,...]

With great functionality, comes great (ir)responsibility!


First assumption: BDH (given (g^a,g^b,g^c), compute $e(g,g)^{abc}$)


Later assumptions: Subgroup Hiding [BGN05], Decision Linear, SXDH


Even later assumptions: q-SDH, q-ADHSDH, q-EDBDH, q-SDH-III, q-SFP, "source group q-parallel BDHE," etc.

Why are q-type assumptions worrisome?

Why are q-type assumptions worrisome?

IBE universe

Alice	Fred	Kate	Phil
Bob	George	Louise	Quentin
Charles	Hannah	Melissa	Rachel
Dora	Isabelle	Nicholas	Sarah
Ernie	Julian	Otis	Tristan

Why are q-type assumptions worrisome?

IBE universe

Alice	Fred	Kate	Phil
Bob	George	Louise	Quentin
Charles	Hannah	Melissa	Rachel
Dora	Isabelle	Nicholas	Sarah
Ernie	Julian	Otis	Tristan

Why are q-type assumptions worrisome?

IBE universe

BDH ⇒

Alice	Fred	Kate	Phil
Bob	George	Louise	Quentin
Charles	Hannah	Melissa	Rachel
Dora	Isabelle	Nicholas	Sarah
Ernie	Julian	Otis	Tristan

Why are q-type assumptions worrisome?

IBE universe

BDH ⇒

Alice	Fred	Kate	Phil	Ursula
Bob	George	Louise	Quentin	Vanessa
Charles	Hannah	Melissa	Rachel	William
Dora	Isabelle	Nicholas	Sarah	Xavier
Ernie	Julian	Otis	Tristan	Yevgeniy

Why are q-type assumptions worrisome?

IBE universe

BDH ⇒ 

Alice	Fred	Kate	Phil	Ursula
Bob	George	Louise	Quentin	Vanessa
Charles	Hannah	Melissa	Rachel	William
Dora	Isabelle	Nicholas	Sarah	Xavier
Ernie	Julian	Otis	Tristan	Yevgeniy

Why are q-type assumptions worrisome?

IBE universe

BDH  $\Rightarrow$

Alice	Fred	Kate	Phil	Ursula
Bob	George	Louise	Quentin	Vanessa
Charles	Hannah	Melissa	Rachel	William
Dora	Isabelle	Nicholas	Sarah	Xavier
Ernie	Julian	Otis	Tristan	Yevgeniy

$(g, g^{x}, \ldots, g^{x^q})$

q-SDH $\Rightarrow$

Alice	Fred	Kate	Phil
Bob	George	Louise	Quentin
Charles	Hannah	Melissa	Rachel
Dora	Isabelle	Nicholas	Sarah
Ernie	Julian	Otis	Tristan

Why are q-type assumptions worrisome?

IBE universe

BDH  $\Rightarrow$

Alice
Bob
Charles
Dora
Ernie

Fred
George
Hannah
Isabelle
Julian

Kate
Louise
Melissa
Nicholas
Otis

Phil
Quentin
Rachel
Sarah
Tristan

Ursula
Vanessa
William
Xavier
Yevgeniy

$(g, g^x, \ldots, g^{x^q})$

q-SDH $\Rightarrow$

Alice
Bob
Charles
Dora
Ernie

Fred
George
Hannah
Isabelle
Julian

Kate
Louise
Melissa
Nicholas
Otis

Phil
Quentin
Rachel
Sarah
Tristan

Ursula
Vanessa
William
Xavier
Yevgeniy

Why are q-type assumptions worrisome?

IBE universe

BDH $\Rightarrow$

Alice Bob Charles Dora Ernie
Fred George Hannah Isabelle Julian
Kate Louise Melissa Nicholas Otis
Phil Quentin Rachel Sarah Tristan
Ursula Vanessa William Xavier Yevgeniy

$(g, g^x, \ldots, g^{x^q})$

q-SDH $\not\Rightarrow$

Alice Bob Charles Dora Ernie
Fred George Hannah Isabelle Julian
Kate Louise Melissa Nicholas Otis
Phil Quentin Rachel Sarah Tristan
Ursula Vanessa William Xavier Yevgeniy

Why are q-type assumptions worrisome?

IBE universe

BDH $\Rightarrow$

Alice
Bob
Charles
Dora
Ernie

Fred
George
Hannah
Isabelle
Julian

Kate
Louise
Melissa
Nicholas
Otis

Phil
Quentin
Rachel
Sarah
Tristan

Ursula
Vanessa
William
Xavier
Yevgeniy

$(g, g^x, \ldots, g^{x^q})$

q-SDH $\not\Rightarrow$

q+5-SDH $\Rightarrow$

$(g, g^x, \ldots, g^{x^q}, \ldots, g^{x^{q+5}})$

Alice
Bob
Charles
Dora
Ernie

Fred
George
Hannah
Isabelle
Julian

Kate
Louise
Melissa
Nicholas
Otis

Phil
Quentin
Rachel
Sarah
Tristan

Ursula
Vanessa
William
Xavier
Yevgeniy

Why are q-type assumptions worrisome?

IBE universe

BDH $\Rightarrow$

Alice Bob Charles Dora Ernie
Fred George Hannah Isabelle Julian
Kate Louise Melissa Nicholas Otis
Phil Quentin Rachel Sarah Tristan
Ursula Vanessa William Xavier Yevgeniy

$(g, g^x, \ldots, g^{x^q})$

q-SDH $\not\Rightarrow$

$\wedge$

q+5-SDH $\Rightarrow$

$(g, g^x, \ldots, g^{x^q}, \ldots, g^{x^{q+5}})$

Alice Bob Charles Dora Ernie
Fred George Hannah Isabelle Julian
Kate Louise Melissa Nicholas Otis
Phil Quentin Rachel Sarah Tristan
Ursula Vanessa William Xavier Yevgeniy

Why are q-type assumptions worrisome?

IBE universe

BDH $\Rightarrow$

Alice	Fred	Kate	Phil	Ursula
Bob	George	Louise	Quentin	Vanessa
Charles	Hannah	Melissa	Rachel	William
Dora	Isabelle	Nicholas	Sarah	Xavier
Ernie	Julian	Otis	Tristan	Yevgeniy

$t/\sqrt{q}$ steps [Cheon06]

q-SDH $\not\Rightarrow$

Alice	Fred	Kate	Phil	Ursula
Bob	George	Louise	Quentin	Vanessa
Charles	Hannah	Melissa	Rachel	William
Dora	Isabelle	Nicholas	Sarah	Xavier
Ernie	Julian	Otis	Tristan	Yevgeniy

$\wedge$

q+5-SDH $\Rightarrow$

$t/\sqrt{q+5}$ steps

Moving away from q-type assumptions

Dual systems [W09,…] have proved effective at removing q-type assumptions

Moving away from q-type assumptions

Dual systems [W09,…] have proved effective at removing q-type assumptions

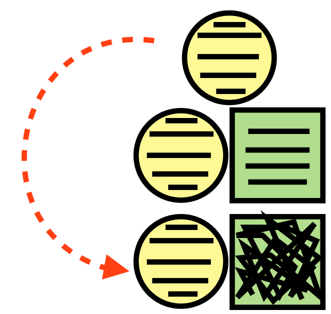
- Properties of bilinear groups: subgroup hiding and parameter hiding

Moving away from q-type assumptions

Dual systems [W09,…] have proved effective at removing q-type assumptions

- Properties of bilinear groups: subgroup hiding and parameter hiding

- Abstract dual systems into three steps

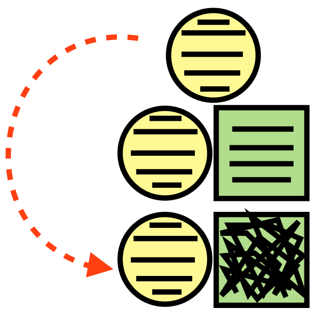


Moving away from q-type assumptions

Dual systems [W09,…] have proved effective at removing q-type assumptions

- Properties of bilinear groups: subgroup hiding and parameter hiding

- Abstract dual systems into three steps



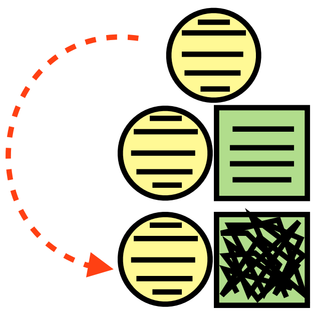
Apply dual systems directly to variants of the uber-assumption [BBG05,B08]

Moving away from q-type assumptions

Dual systems [W09,…] have proved effective at removing q-type assumptions

- Properties of bilinear groups: subgroup hiding and parameter hiding

- Abstract dual systems into three steps



Apply dual systems directly to variants of the uber-assumption [BBG05,B08]

- Reduce* to an assumption that holds by a statistical argument

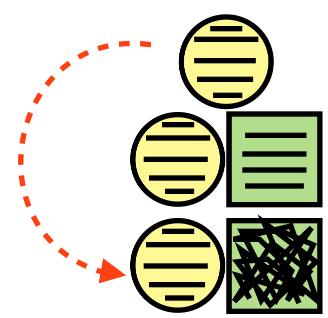
*currently only in composite-order groups

Moving away from q-type assumptions

Dual systems [W09,…] have proved effective at removing q-type assumptions

- Properties of bilinear groups: subgroup hiding and parameter hiding

- Abstract dual systems into three steps



Apply dual systems directly to variants of the uber-assumption [BBG05,B08]

- Reduce* to an assumption that holds by a statistical argument
- Adapt dual systems to work for deterministic primitives

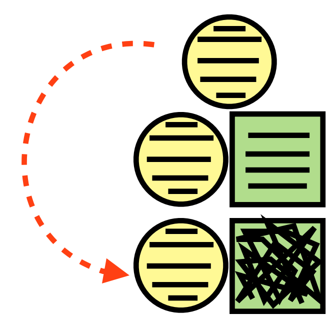
*currently only in composite-order groups

Moving away from q-type assumptions

Dual systems [W09,…] have proved effective at removing q-type assumptions

- Properties of bilinear groups: subgroup hiding and parameter hiding

- Abstract dual systems into three steps



Apply dual systems directly to variants of the uber-assumption [BBG05,B08]

- Reduce* to an assumption that holds by a statistical argument
- Adapt dual systems to work for deterministic primitives

Extension to Dodis-Yampolskiy PRF [DY05]

*currently only in composite-order groups

Outline

Outline

Bilinear groups

Outline

Bilinear groups

q-Type assumptions

Outline

Bilinear groups

q-Type assumptions

Extensions

Outline

Bilinear groups	q-Type assumptions
Extensions	Conclusions

Outline

Bilinear groups
Subgroup hiding
Parameter hiding
Dual systems

q-Type assumptions

Extensions

Conclusions

Properties of (bilinear) groups

Standard bilinear group: (N, G, H, G_T, e, g, h)

Properties of (bilinear) groups

Standard bilinear group: (N, G, H, G_T, e, g, h)

Group order;
prime or composite

Properties of (bilinear) groups

Standard bilinear group: $(N, \underbrace{G, H, G_T}_{|G| = |H| = \kappa N;\ |G_T| = \lambda N}, e, g, h)$

Group order; prime or composite

$|G| = |H| = \kappa N$; $|G_T| = \lambda N$

Properties of (bilinear) groups

Standard bilinear group: $(N, \underbrace{G, H, G_T}, e, g, h)$

Group order;
prime or composite

$|G| = |H| = \kappa N$; $|G_T| = \lambda N$

$e: G \times H \to G_T$

bilinearity: $e(g^a,h^b) = e(g,h)^{ab}$ $\forall a,b \in Z/NZ$

non-degeneracy: $e(x,y) = 1$ $\forall y \in H \Rightarrow x = 1$

Properties of (bilinear) groups

Standard bilinear group: (N, G, H, G_T, e, g, h)

Group order;
prime or composite

G = <g>; H = <h>

$|G| = |H| = \kappa N$; $|G_T| = \lambda N$

$e: G \times H \to G_T$

bilinearity: $e(g^a,h^b) = e(g,h)^{ab}$ $\forall a,b \in Z/NZ$

non-degeneracy: $e(x,y) = 1$ $\forall y \in H \Rightarrow x = 1$

Properties of (bilinear) groups

Standard bilinear group: (N, G, H, G_T, e, g, h)

Group order;
prime or composite

$|G| = |H| = \kappa N$; $|G_T| = \lambda N$

$G = \langle g \rangle$; $H = \langle h \rangle$

$e: G \times H \to G_T$

bilinearity: $e(g^a,h^b) = e(g,h)^{ab}$ $\forall a,b \in Z/NZ$

non-degeneracy: $e(x,y) = 1$ $\forall y \in H \Rightarrow x = 1$

Properties of (bilinear) groups

Standard bilinear group: (N, G, H, G_T, e, g, h)

Group order; prime or composite

$|G| = |H| = \kappa N$; $|G_T| = \lambda N$

$G = \langle g \rangle$; $H = \langle h \rangle$

$e: G \times H \to G_T$

bilinearity: $e(g^a, h^b) = e(g,h)^{ab}$ $\forall a,b \in Z/NZ$

non-degeneracy: $e(x,y) = 1$ $\forall y \in H \Rightarrow x = 1$

subgroup hiding

Properties of (bilinear) groups

Standard bilinear group: (N, G, H, G_T, e, g, h)

Group order;
prime or composite

$|G| = |H| = \kappa N$; $|G_T| = \lambda N$

$G = \langle g \rangle$; $H = \langle h \rangle$

$e: G \times H \rightarrow G_T$

bilinearity: $e(g^a, h^b) = e(g,h)^{ab}\ \forall a,b \in \mathbb{Z}/N\mathbb{Z}$

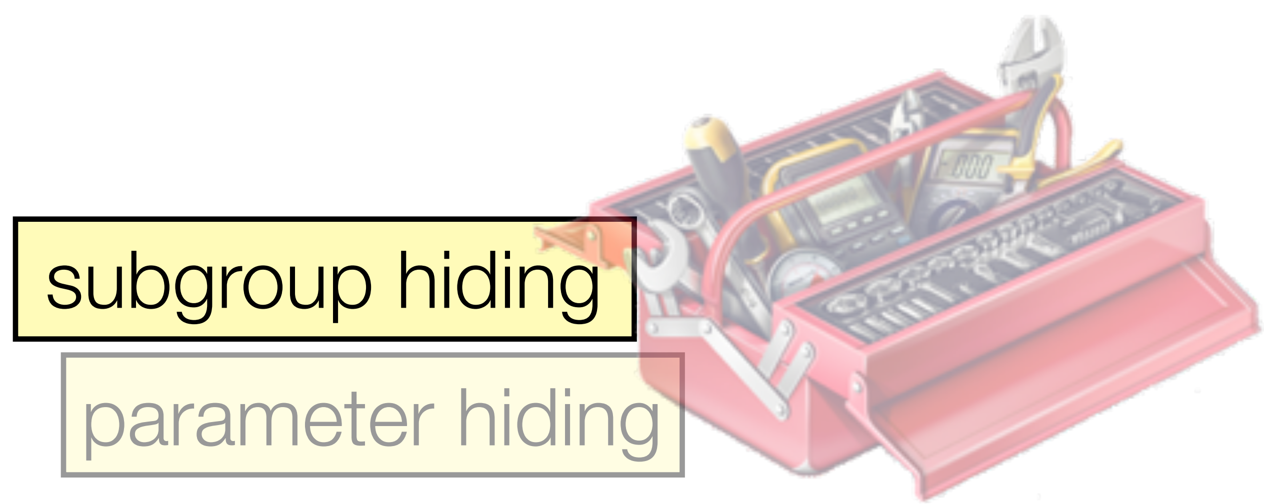
non-degeneracy: $e(x,y) = 1\ \forall y \in H \Rightarrow x = 1$

subgroup hiding

parameter hiding

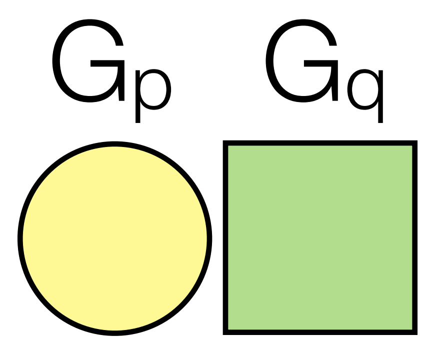
Subgroup hiding

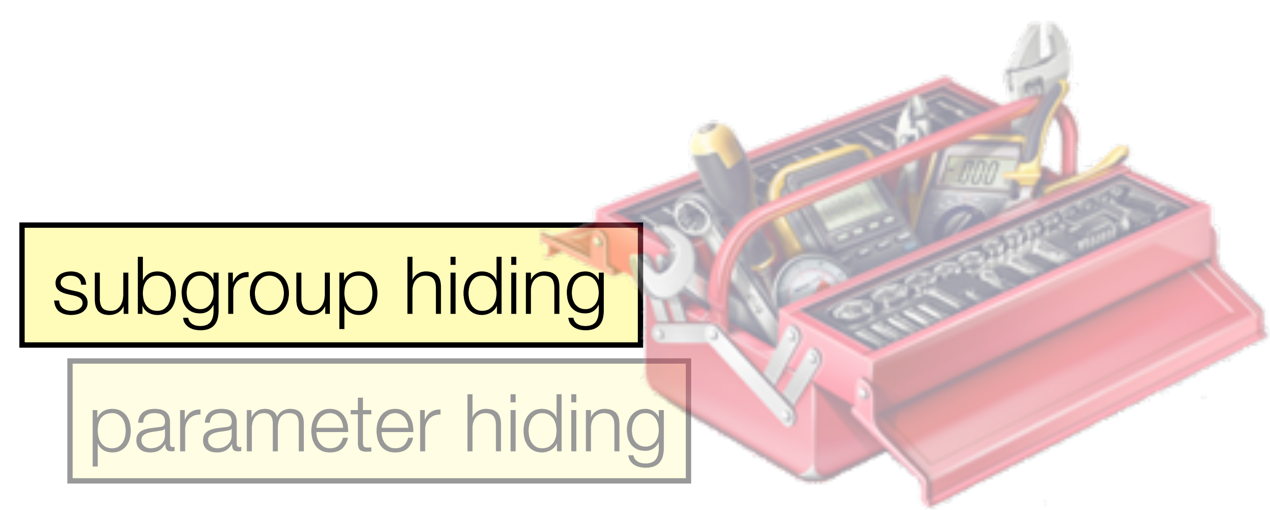
Composite-order bilinear group: (N, G, G_T, e, g) where $N = pq$



Subgroup hiding

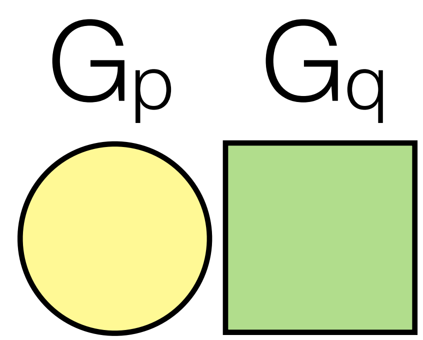
Composite-order bilinear group: (N, G, G_T, e, g) where $N = pq$



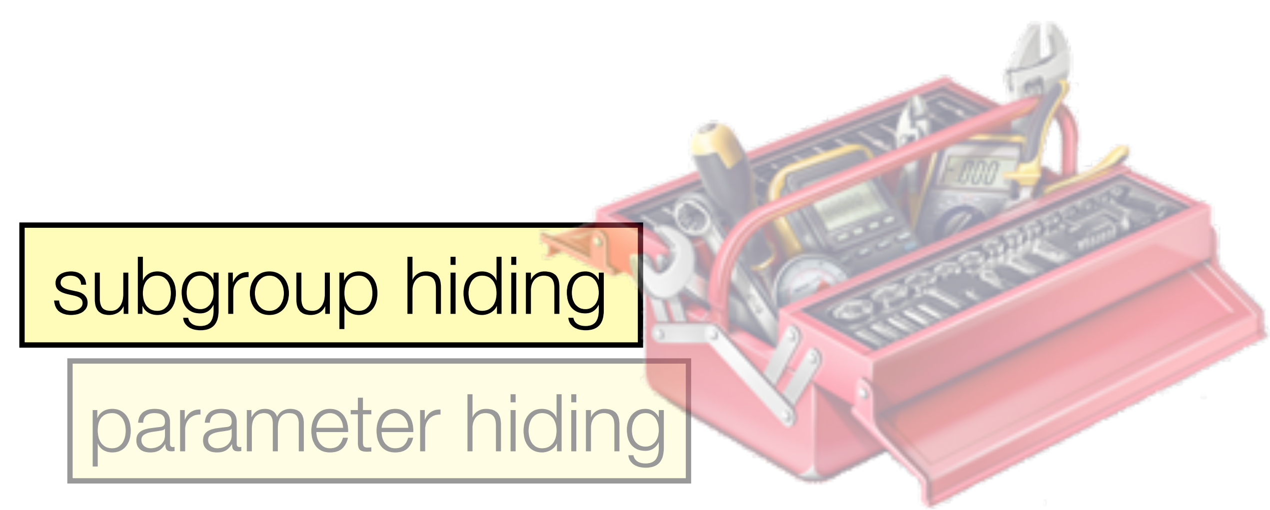


Subgroup hiding

Composite-order bilinear group: (N, G, G_T, e, g) where $N = pq$

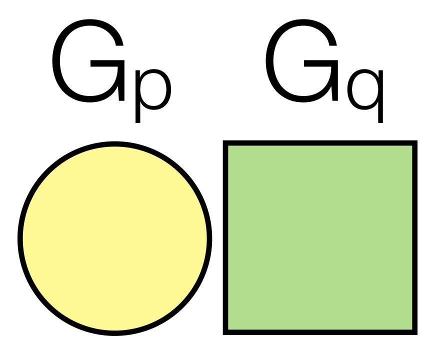


Subgroup hiding [BGN05]:

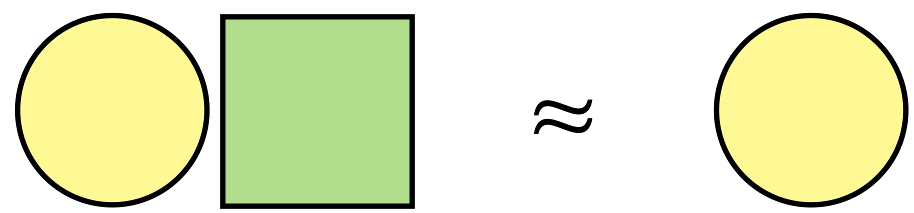


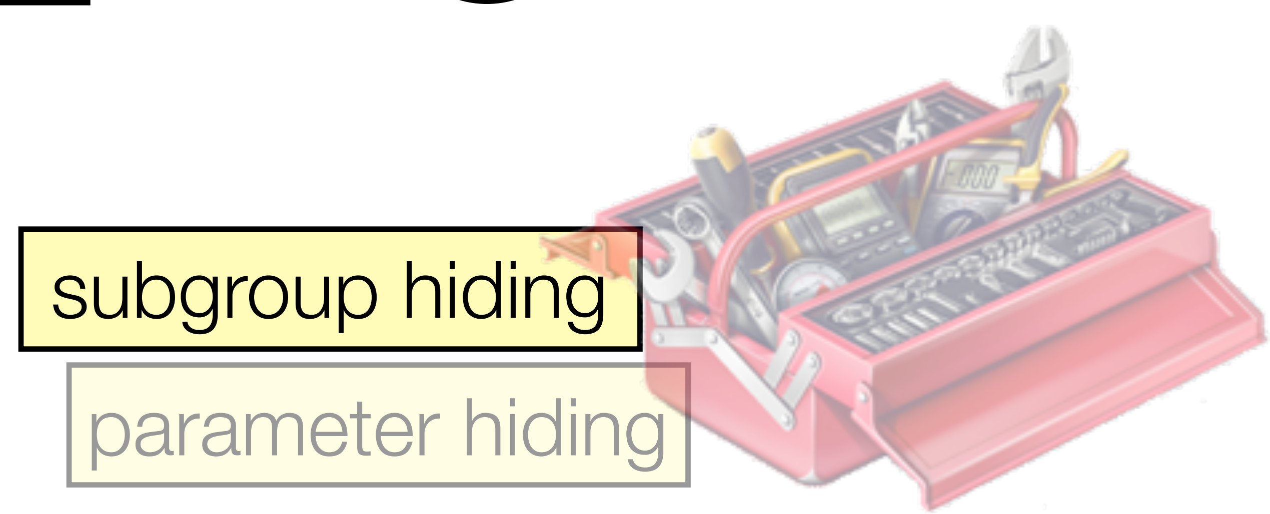
Subgroup hiding

Composite-order bilinear group: (N, G, G_T, e, g) where $N = pq$



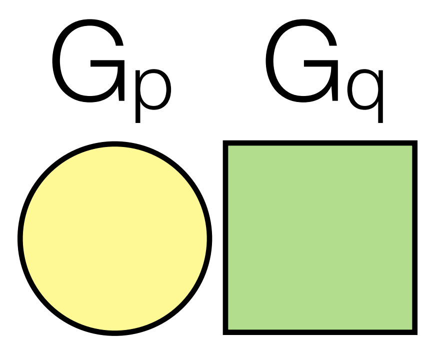
Subgroup hiding [BGN05]:



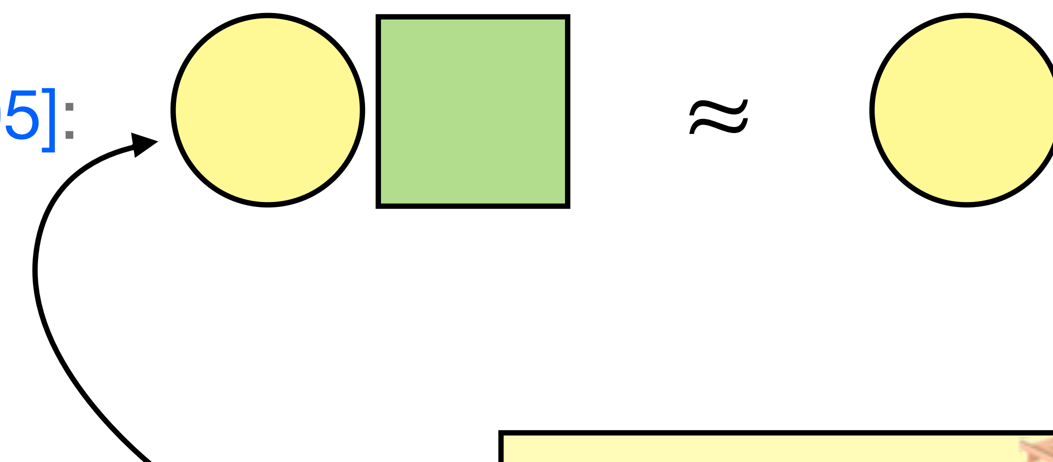


Subgroup hiding

Composite-order bilinear group: (N, G, G_T, e, g) where $N = pq$



Subgroup hiding [BGN05]:



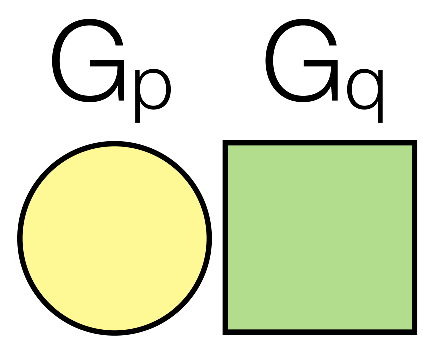
random element of $G_p \times G_q$

subgroup hiding

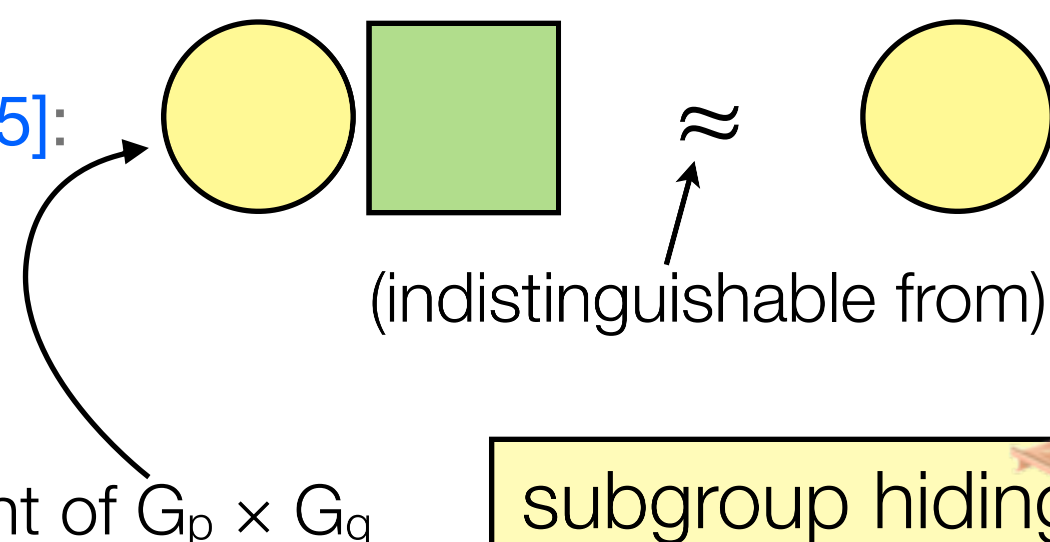
parameter hiding

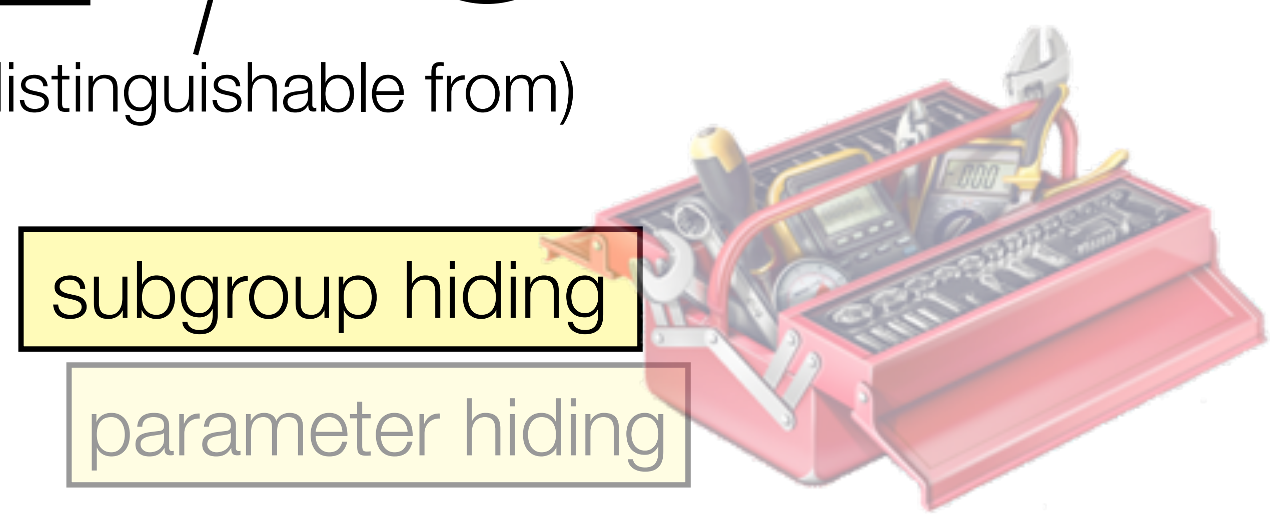
Subgroup hiding

Composite-order bilinear group: (N, G, G_T, e, g) where $N = pq$



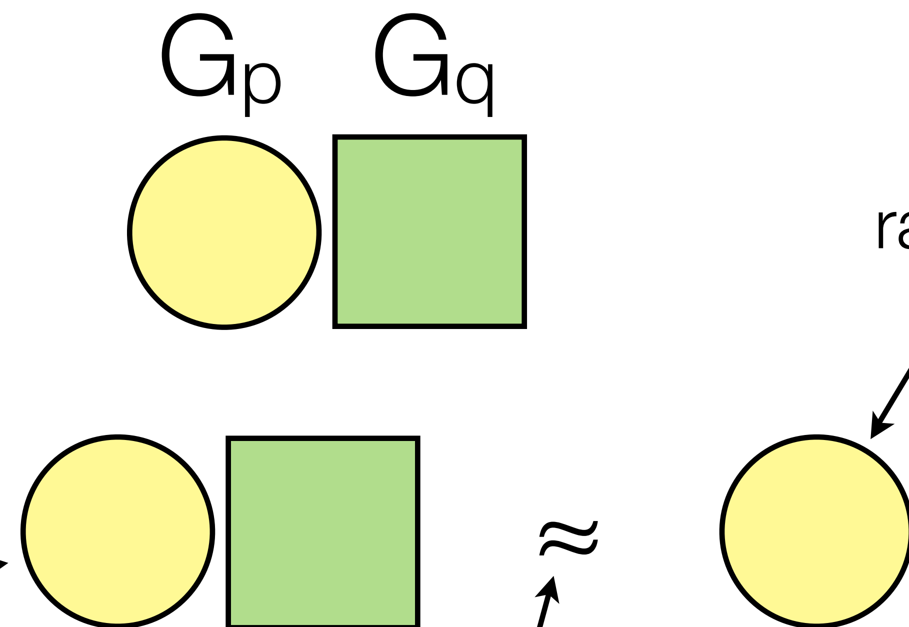
Subgroup hiding [BGN05]:





Subgroup hiding

Composite-order bilinear group: (N, G, G_T, e, g) where $N = pq$



random element of G_p

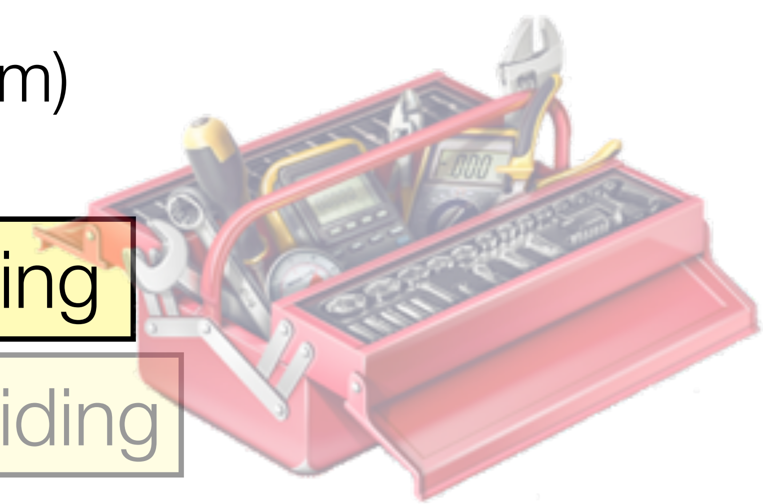
Subgroup hiding [BGN05]:

(indistinguishable from)

random element of $G_p \times G_q$

subgroup hiding

parameter hiding

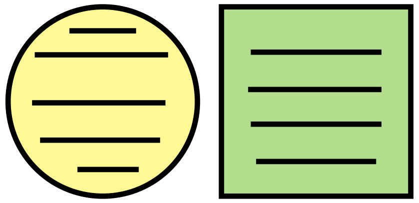


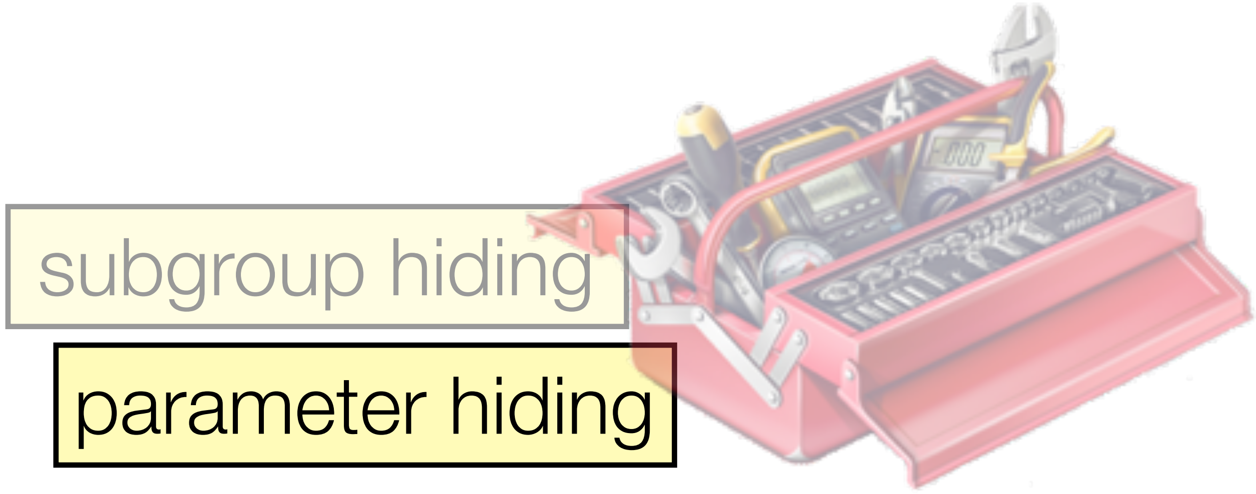
Parameter hiding [L12]

Parameter hiding: elements correlated across subgroups are distributed identically to uncorrelated elements

Parameter hiding [L12]

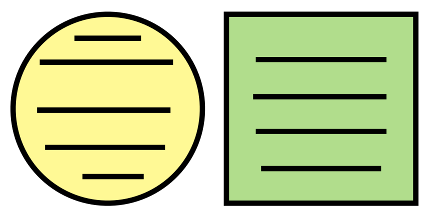
Parameter hiding: elements correlated across subgroups are distributed identically to uncorrelated elements





Parameter hiding [L12]

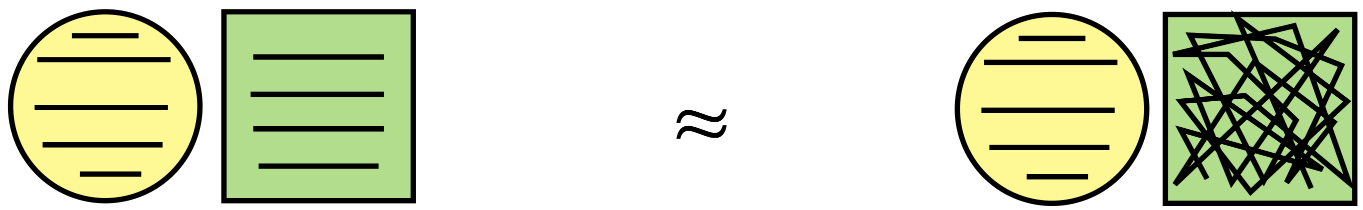
Parameter hiding: elements correlated across subgroups are distributed identically to uncorrelated elements



$$g_1^{f(x_1,\ldots,x_c)} g_2^{f(x_1,\ldots,x_c)}$$

Parameter hiding [L12]

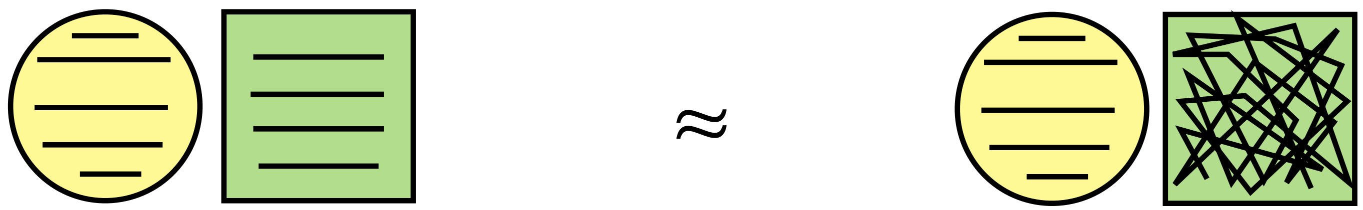
Parameter hiding: elements correlated across subgroups are distributed identically to uncorrelated elements



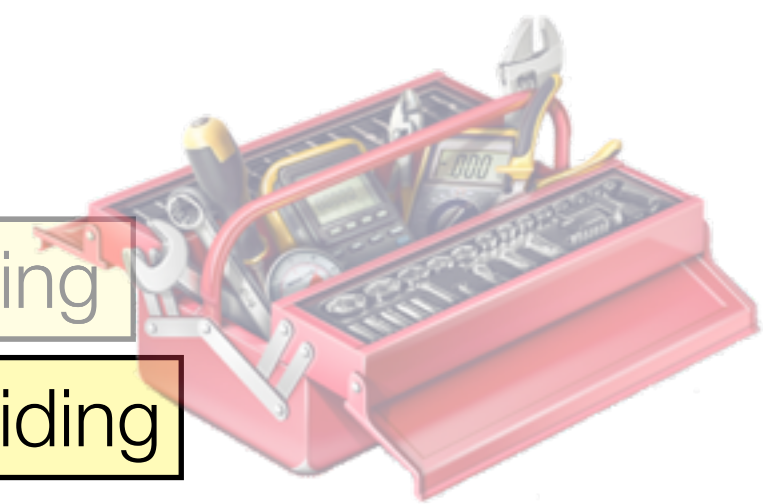
$$g_1^{f(x_1,\ldots,x_C)} g_2^{f(x_1,\ldots,x_C)}$$

Parameter hiding [L12]

Parameter hiding: elements correlated across subgroups are distributed identically to uncorrelated elements



$$g_1^{f(x_1,\dots,x_c)} g_2^{f(x_1,\dots,x_c)} \approx g_1^{f(x_1,\dots,x_c)} g_2^{f(x_1',\dots,x_c')}$$

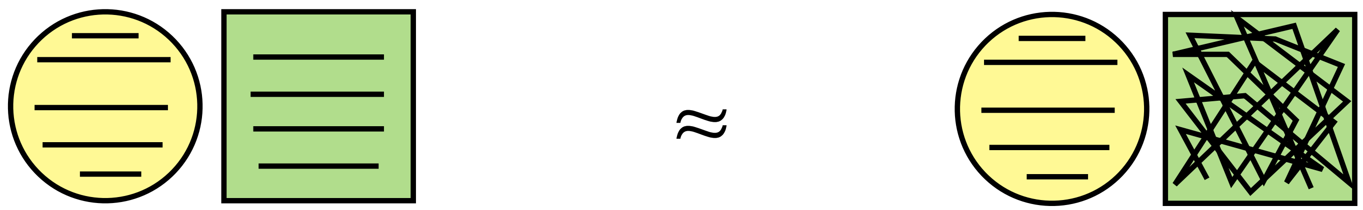


subgroup hiding

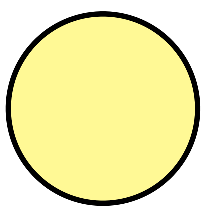
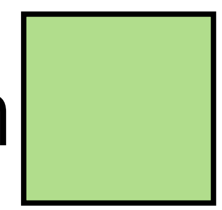
parameter hiding

Parameter hiding [L12]

Parameter hiding: elements correlated across subgroups are distributed identically to uncorrelated elements

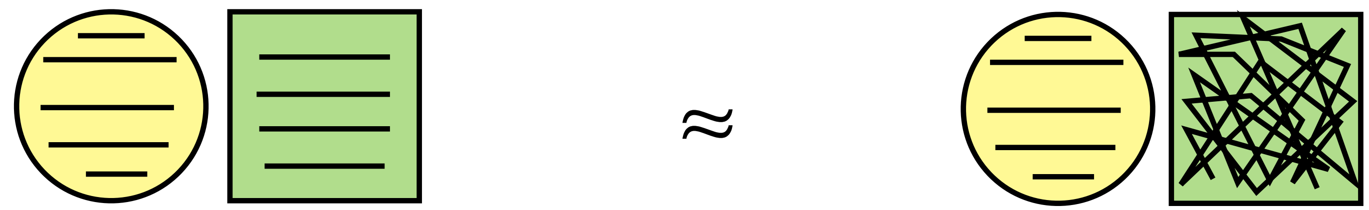


$$g_1^{f(x_1,\dots,x_c)} g_2^{f(x_1,\dots,x_c)} \approx g_1^{f(x_1,\dots,x_c)} g_2^{f(x_1',\dots,x_c')}$$

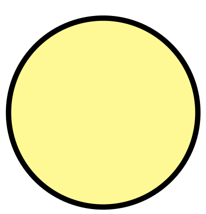
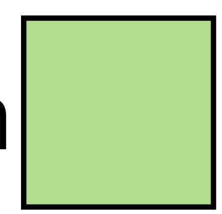
 is independent from 

Parameter hiding [L12]

Parameter hiding: elements correlated across subgroups are distributed identically to uncorrelated elements



$$g_1^{f(x_1,\dots,x_c)} g_2^{f(x_1,\dots,x_c)} \approx g_1^{f(x_1,\dots,x_c)} g_2^{f(x_1',\dots,x_c')}$$

 is independent from 

x_i mod p reveals nothing about x_i mod q (CRT)

Typical dual-system proof for IBE [W09,LW10,...]

Typical dual-system proof for IBE [W09,LW10,...]

Challenge ciphertext

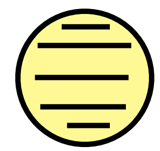
Typical dual-system proof for IBE [W09,LW10,...]

Challenge ciphertext

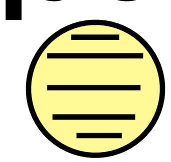
ID queries

Typical dual-system proof for IBE [W09,LW10,...]

Challenge ciphertext

normal: 

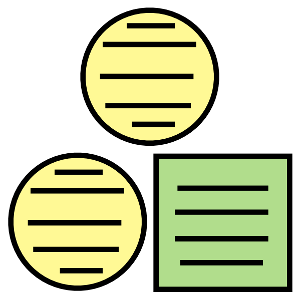
ID queries

normal: 

Typical dual-system proof for IBE [W09,LW10,...]

Challenge ciphertext

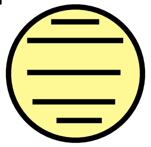
normal:



(subgroup hiding)

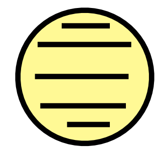
ID queries

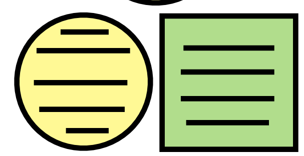
normal:

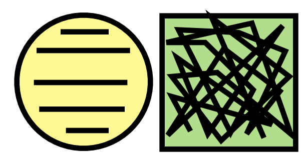


Typical dual-system proof for IBE [W09,LW10,...]

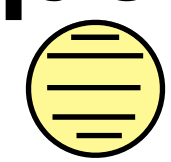
Challenge ciphertext

normal: 

 (subgroup hiding)

 (parameter hiding)

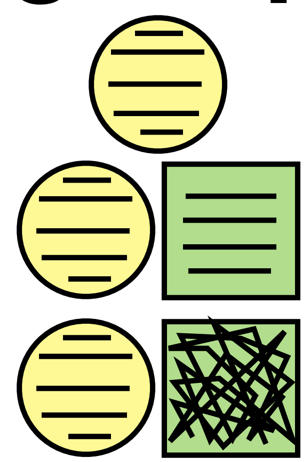
ID queries

normal: 

Typical dual-system proof for IBE [W09,LW10,...]

Challenge ciphertext

normal:



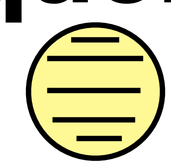
(subgroup hiding)

semi-functional (SF):

(parameter hiding)

ID queries

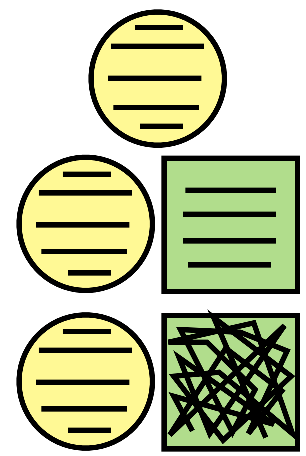
normal:



Typical dual-system proof for IBE [W09,LW10,...]

Challenge ciphertext

normal:



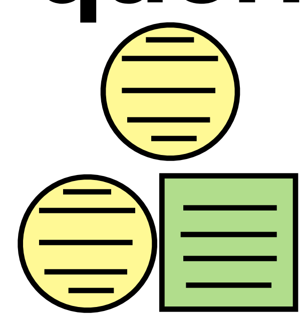
(subgroup hiding)

semi-functional (SF):

(parameter hiding)

ID queries

normal:

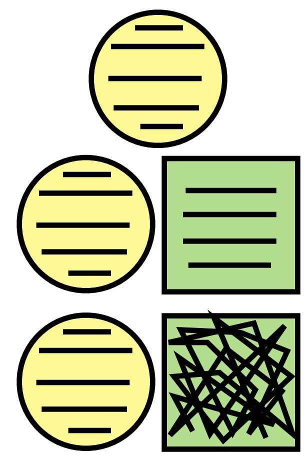


(subgroup hiding)

Typical dual-system proof for IBE [W09,LW10,...]

Challenge ciphertext

normal:



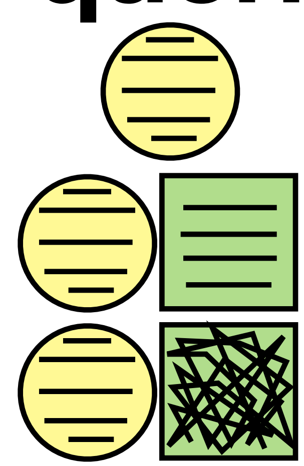
(subgroup hiding)

semi-functional (SF):

(parameter hiding)

ID queries

normal:



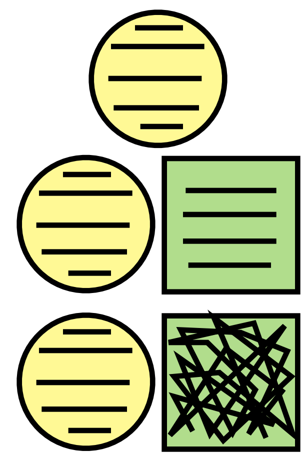
(subgroup hiding)

(parameter hiding)

Typical dual-system proof for IBE [W09,LW10,...]

Challenge ciphertext

normal:



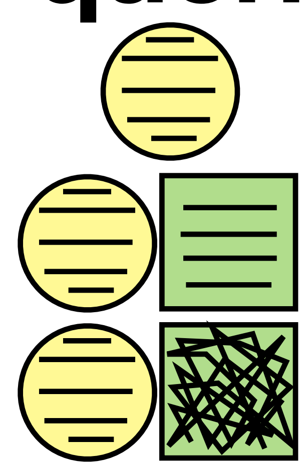
(subgroup hiding)

semi-functional (SF):

(parameter hiding)

ID queries

normal:



(subgroup hiding)

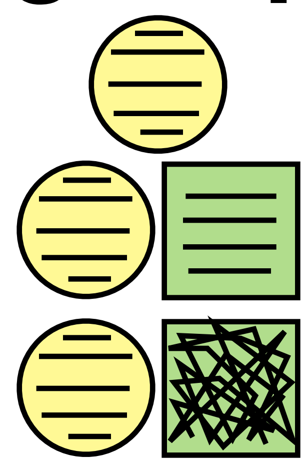
semi-functional (SF):

(parameter hiding)

Typical dual-system proof for IBE [W09,LW10,...]

Challenge ciphertext

normal:



(subgroup hiding)

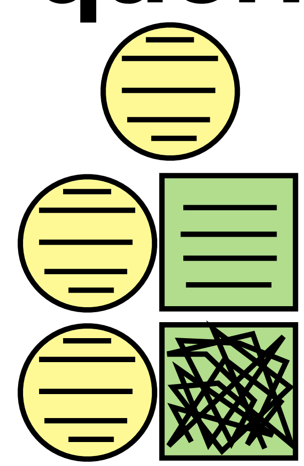
semi-functional (SF):

(parameter hiding)

SF keys don't decrypt SF ciphertexts!

ID queries

normal:



(subgroup hiding)

semi-functional (SF):

(parameter hiding)

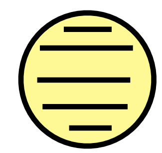
Dual systems in three easy steps

Dual systems in three easy steps

1. start with base scheme

Dual systems in three easy steps

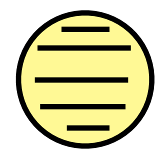
normal:



1. start with base scheme

Dual systems in three easy steps

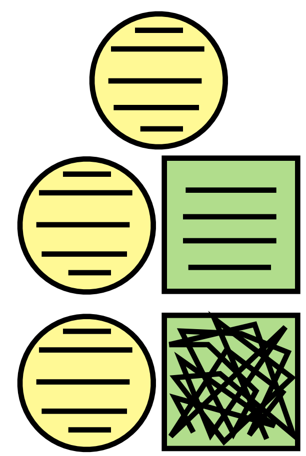
normal:



1. start with base scheme
2. transition to SF version

Dual systems in three easy steps

normal:



(subgroup hiding)

semi-functional (SF):

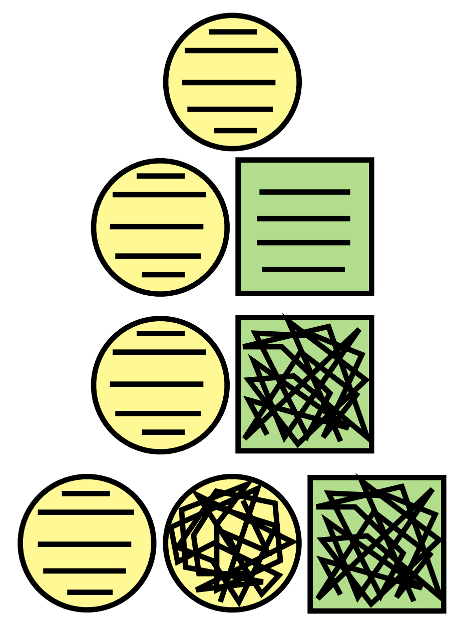
(parameter hiding)

1. start with base scheme
2. transition to SF version

Dual systems in three easy steps

normal:

semi-functional (SF):



(subgroup hiding)

(parameter hiding)

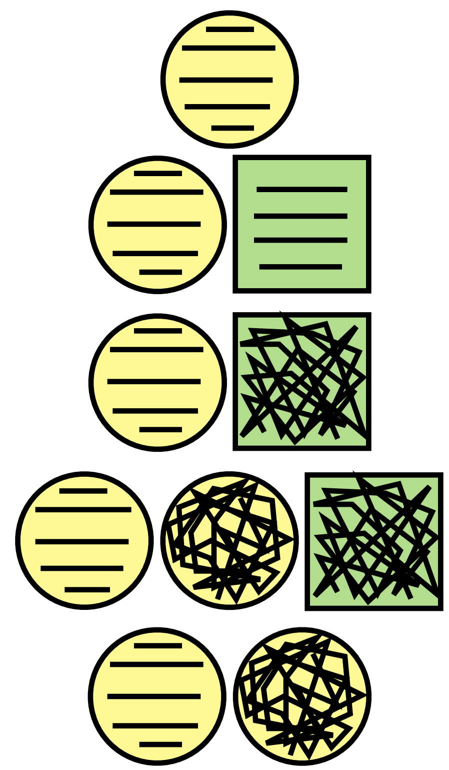
(subgroup hiding)

1. start with base scheme
2. transition to SF version

Dual systems in three easy steps

normal:

semi-functional (SF):



(subgroup hiding)

(parameter hiding)

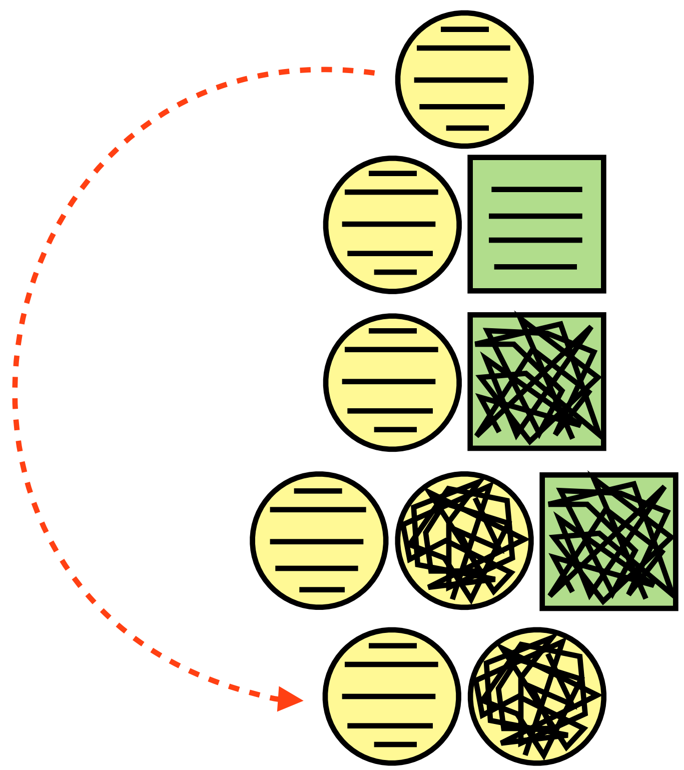
(subgroup hiding)

(subgroup hiding)

1. start with base scheme
2. transition to SF version

Dual systems in three easy steps

normal:



(subgroup hiding)

(parameter hiding)

(subgroup hiding)

semi-functional (SF):

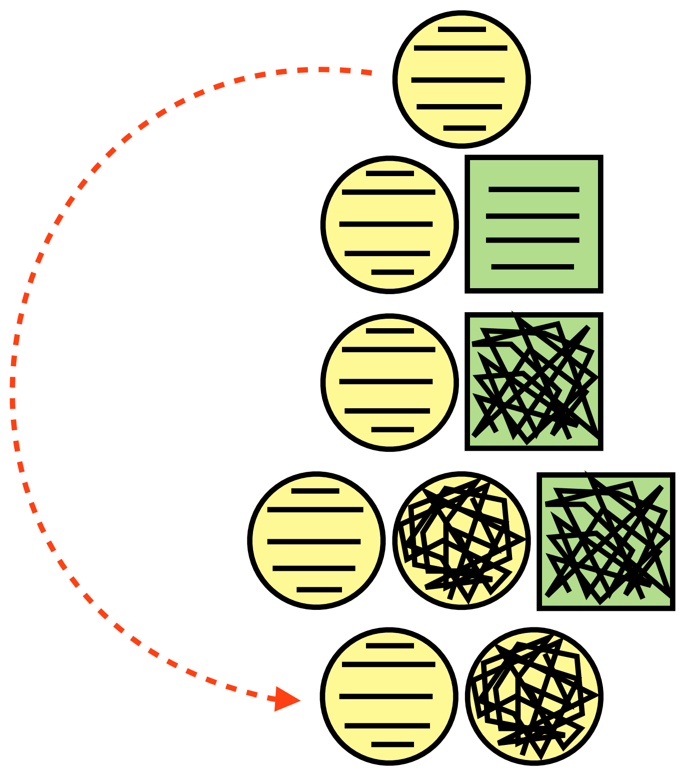
(subgroup hiding)

1. start with base scheme
2. transition to SF version

Dual systems in three easy steps

normal:

semi-functional (SF):



(subgroup hiding)

(parameter hiding)

(subgroup hiding)

(subgroup hiding)

1. start with base scheme
2. transition to SF version
3. argue information is hidden

Outline

Bilinear groups

q-Type assumptions
The uber-assumption
Relating uber-assumptions
A bijection trick

Extensions

Conclusions

The "uber-assumption" [BBG05,B08]

Uber-assumption is parameterized by (c,R,S,T,f)

The “uber-assumption” [BBG05,B08]

Uber-assumption is parameterized by (c,R,S,T,f)

- c = number of variables: $x_1,\ldots,x_c \leftarrow \mathcal{R}$

The “uber-assumption” [BBG05,B08]

Uber-assumption is parameterized by (c,R,S,T,f)

- c = number of variables: $x_1,\ldots,x_c \leftarrow \mathcal{R}$
- $R = <1,\rho_1,\ldots,\rho_r>$: A is given g, $\{g^{\rho_i(x_1,\ldots,x_c)}\}$

The “uber-assumption” [BBG05,B08]

Uber-assumption is parameterized by (c,R,S,T,f)

- c = number of variables: $x_1,\ldots,x_c \leftarrow \mathcal{R}$
- $R = \langle 1,\rho_1,\ldots,\rho_r \rangle$: A is given g, $\{g^{\rho_i(x_1,\ldots,x_c)}\}$
- $S = \langle 1,\sigma_1,\ldots,\sigma_s \rangle$: A is given h, $\{h^{\sigma_i(x_1,\ldots,x_c)}\}$

The "uber-assumption" [BBG05,B08]

Uber-assumption is parameterized by (c,R,S,T,f)

- c = number of variables: $x_1,\ldots,x_c \leftarrow \mathcal{R}$
- $R = \langle 1,\rho_1,\ldots,\rho_r \rangle$: A is given g, $\{g^{\rho_i(x_1,\ldots,x_c)}\}$
- $S = \langle 1,\sigma_1,\ldots,\sigma_s \rangle$: A is given h, $\{h^{\sigma_i(x_1,\ldots,x_c)}\}$
- $T = \langle 1,\tau_1,\ldots,\tau_t \rangle$: A is given e(g,h), $\{e(g,h)^{\tau_i(x_1,\ldots,x_c)}\}$

The “uber-assumption” [BBG05,B08]

Uber-assumption is parameterized by (c,R,S,T,f)

- c = number of variables: $x_1,\ldots,x_c \leftarrow \mathcal{R}$
- $R = <1,\rho_1,\ldots,\rho_r>$: A is given g, $\{g^{\rho_i(x_1,\ldots,x_c)}\}$
- $S = <1,\sigma_1,\ldots,\sigma_s>$: A is given h, $\{h^{\sigma_i(x_1,\ldots,x_c)}\}$
- $T = <1,\tau_1,\ldots,\tau_t>$: A is given e(g,h), $\{e(g,h)^{\tau_i(x_1,\ldots,x_c)}\}$
- $f(x_1,\ldots,x_c)$: A needs to compute $e(g,h)^{f(x_1,\ldots,x_c)}$ (or distinguish it from random)

The “uber-assumption” [BBG05,B08]

Uber-assumption is parameterized by (c,R,S,T,f)

- c = number of variables: $x_1,\ldots,x_c \leftarrow \mathcal{R}$
- R = $<1,\rho_1,\ldots,\rho_r>$: A is given g, $\{g^{\rho_i(x_1,\ldots,x_c)}\}$
- S = $<1,\sigma_1,\ldots,\sigma_s>$: A is given h, $\{h^{\sigma_i(x_1,\ldots,x_c)}\}$
- T = $<1,\tau_1,\ldots,\tau_t>$: A is given e(g,h), $\{e(g,h)^{\tau_i(x_1,\ldots,x_c)}\}$
- $f(x_1,\ldots,x_c)$: A needs to compute $e(g,h)^{f(x_1,\ldots,x_c)}$ (or distinguish it from random)

uber(c,R,S,T,f) assumption: given (R,S,T) values, hard to compute/distinguish f

Example uber-assumption: exponent q-SDH

exponent q-SDH [ZS-NS04]: given $(g,g^x,\ldots,g^{x^q})$, distinguish $g^{x^{q+1}}$ from random

Example uber-assumption: exponent q-SDH

exponent q-SDH [ZS-NS04]: given $(g,g^x,\ldots,g^{x^q})$, distinguish $g^{x^{q+1}}$ from random

- c = number of variables: c = 1

Example uber-assumption: exponent q-SDH

exponent q-SDH [ZS-NS04]: given $(g, g^x, \ldots, g^{x^q})$, distinguish $g^{x^{q+1}}$ from random

- c = number of variables: c = 1
- $R = \langle 1, \rho_1, \ldots, \rho_r \rangle$: $\rho_i(x) = x^i$ $(\forall i\ 0 \leq i \leq q)$

Example uber-assumption: exponent q-SDH

exponent q-SDH [ZS-NS04]: given $(g,g^x,\ldots,g^{x^q})$, distinguish $g^{x^{q+1}}$ from random

- c = number of variables: c = 1
- $R = \langle 1,\rho_1,\ldots,\rho_r \rangle$: $\rho_i(x) = x^i$ ($\forall i$ $0 \leq i \leq q$)
- $S = \langle 1 \rangle$
- $T = \langle 1 \rangle$

Example uber-assumption: exponent q-SDH

exponent q-SDH [ZS-NS04]: given $(g,g^{x},\ldots,g^{x^q})$, distinguish $g^{x^{q+1}}$ from random

- c = number of variables: $c = 1$
- $R = \langle 1,\rho_1,\ldots,\rho_r \rangle$: $\rho_i(x) = x^i$ ($\forall i\ 0 \leq i \leq q$)
- $S = \langle 1 \rangle$
- $T = \langle 1 \rangle$
- $f(x_1,\ldots,x_c)$: $f(x) = x^{q+1}$

Example uber-assumption: exponent q-SDH

exponent q-SDH [ZS-NS04]: given $(g, g^{x}, \ldots, g^{x^q})$, distinguish $g^{x^{q+1}}$ from random

- c = number of variables: $c = 1$
- $R = \langle 1, \rho_1, \ldots, \rho_r \rangle$: $\rho_i(x) = x^i$ ($\forall i\ 0 \leq i \leq q$)
- $S = \langle 1 \rangle$
- $T = \langle 1 \rangle$
- $f(x_1, \ldots, x_c)$: $f(x) = x^{q+1}$

exponent q-SDH is $\mathrm{uber}(1, \langle 1, \{x^i\} \rangle, \langle 1 \rangle, \langle 1 \rangle, x^{q+1})$

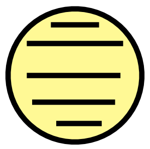
Applying dual systems to exponent q-SDH

$\text{uber}(c, \langle 1, \{x^i\} \rangle, \langle 1 \rangle, \langle 1 \rangle, x^{q+1})$

1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to exponent q-SDH

$\text{uber}(c,<1,\{x^i\}>,<1>,<1>,x^{q+1})$

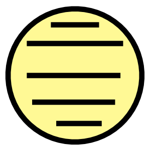


$g_1^{r_1x_1},\ldots,g_1^{r_1x_1^q}$

1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to exponent q-SDH

$\mathrm{uber}(c,\langle 1,\{x^i\}\rangle,\langle 1\rangle,\langle 1\rangle,x^{q+1})$

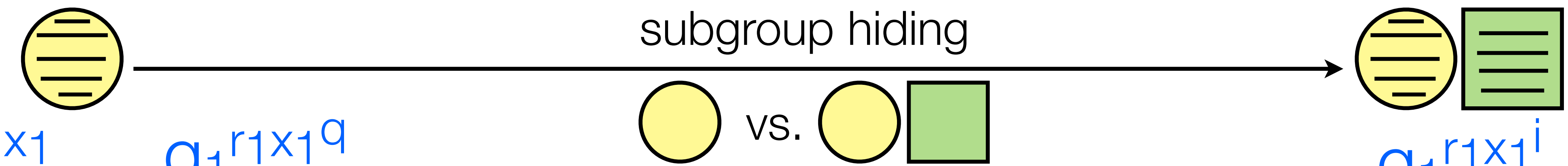


$g_1^{r_1x_1},\ldots,g_1^{r_1x_1^q}$

1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to exponent q-SDH

$\mathrm{uber}(c,\langle 1,\{x^i\}\rangle,\langle 1\rangle,\langle 1\rangle,x^{q+1})$

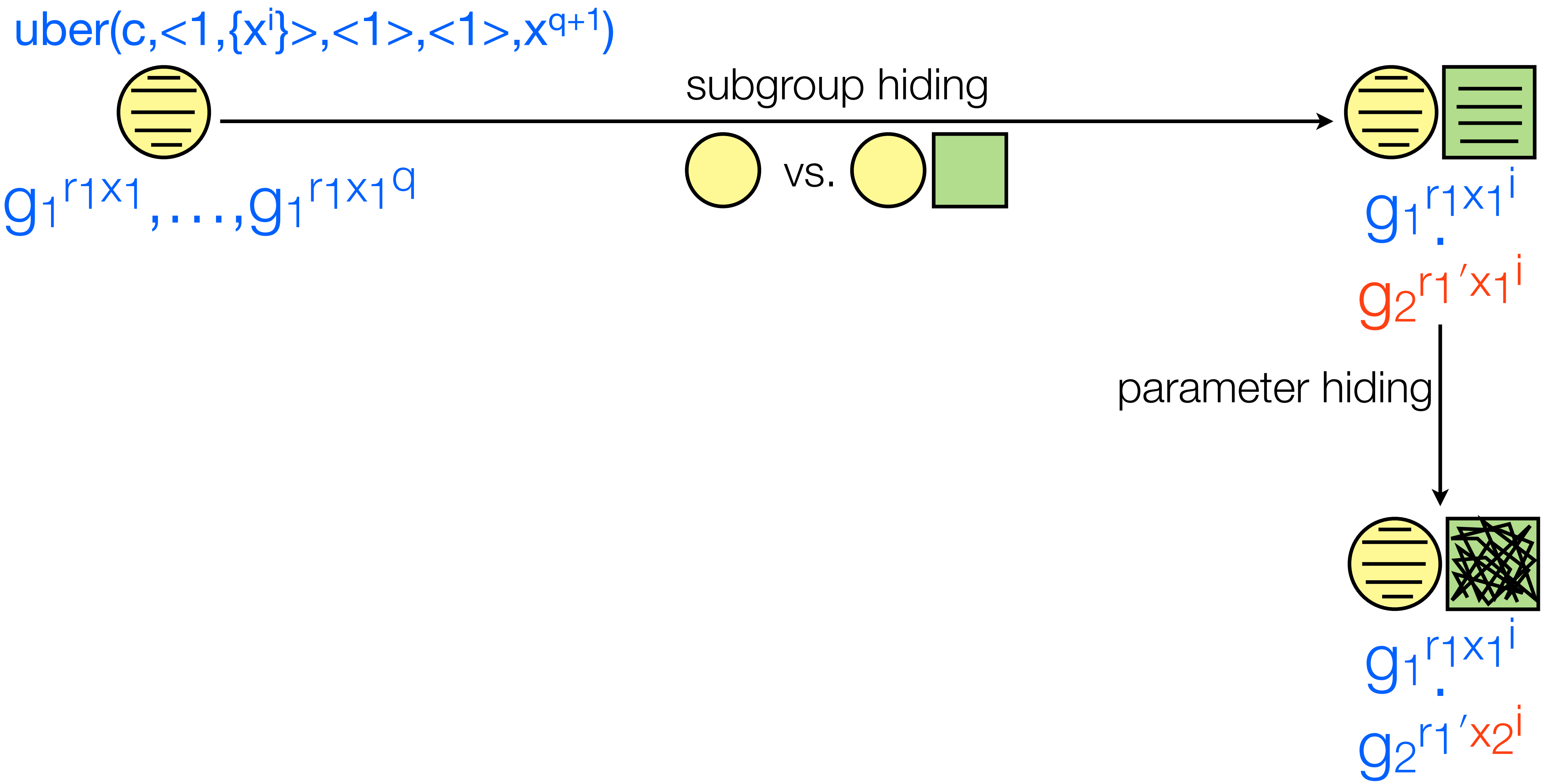


$g_1^{r_1 x_1}, \ldots, g_1^{r_1 x_1^q}$

$g_1^{r_1 x_1^i} \cdot g_2^{r_1' x_1^i}$

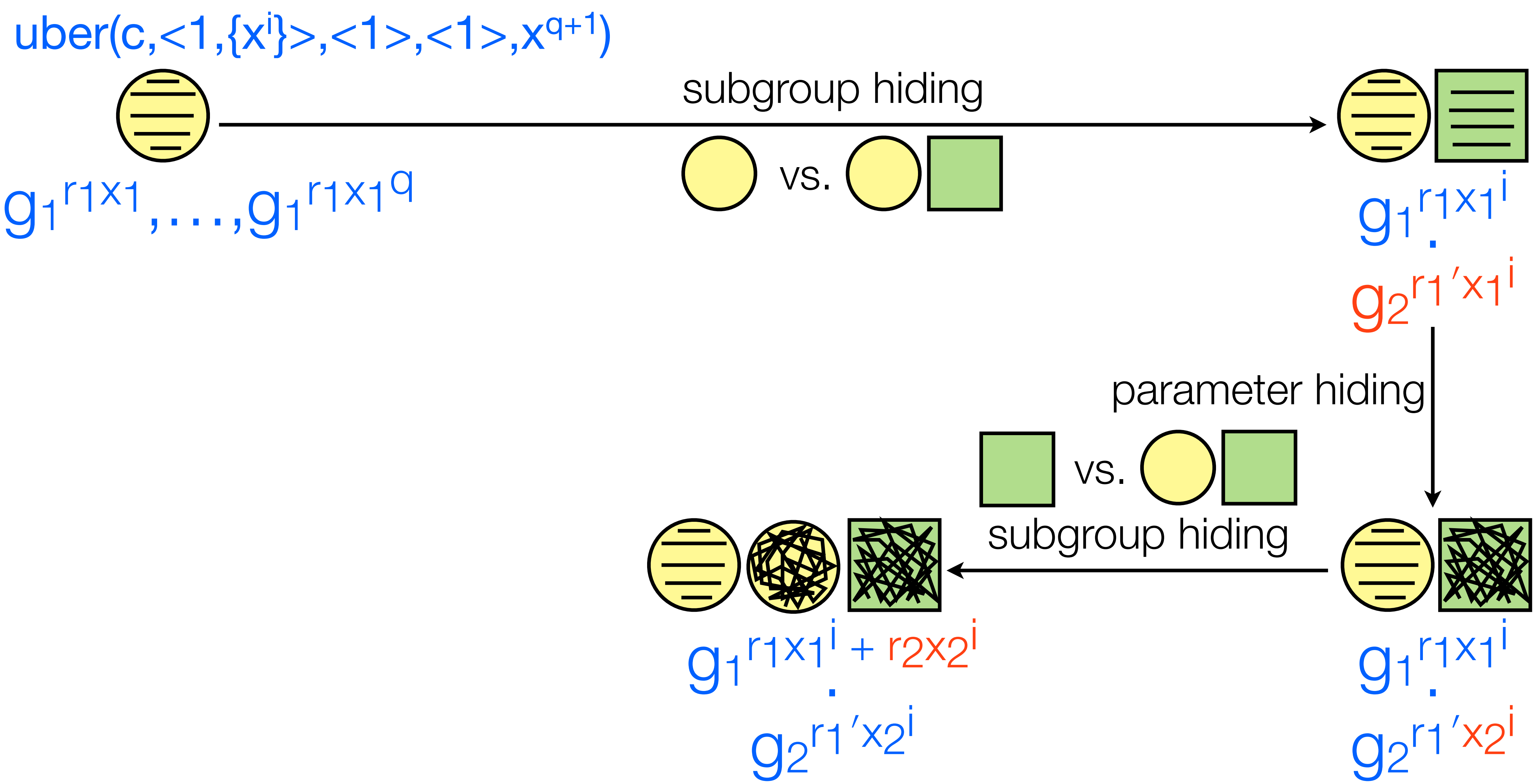
1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to exponent q-SDH



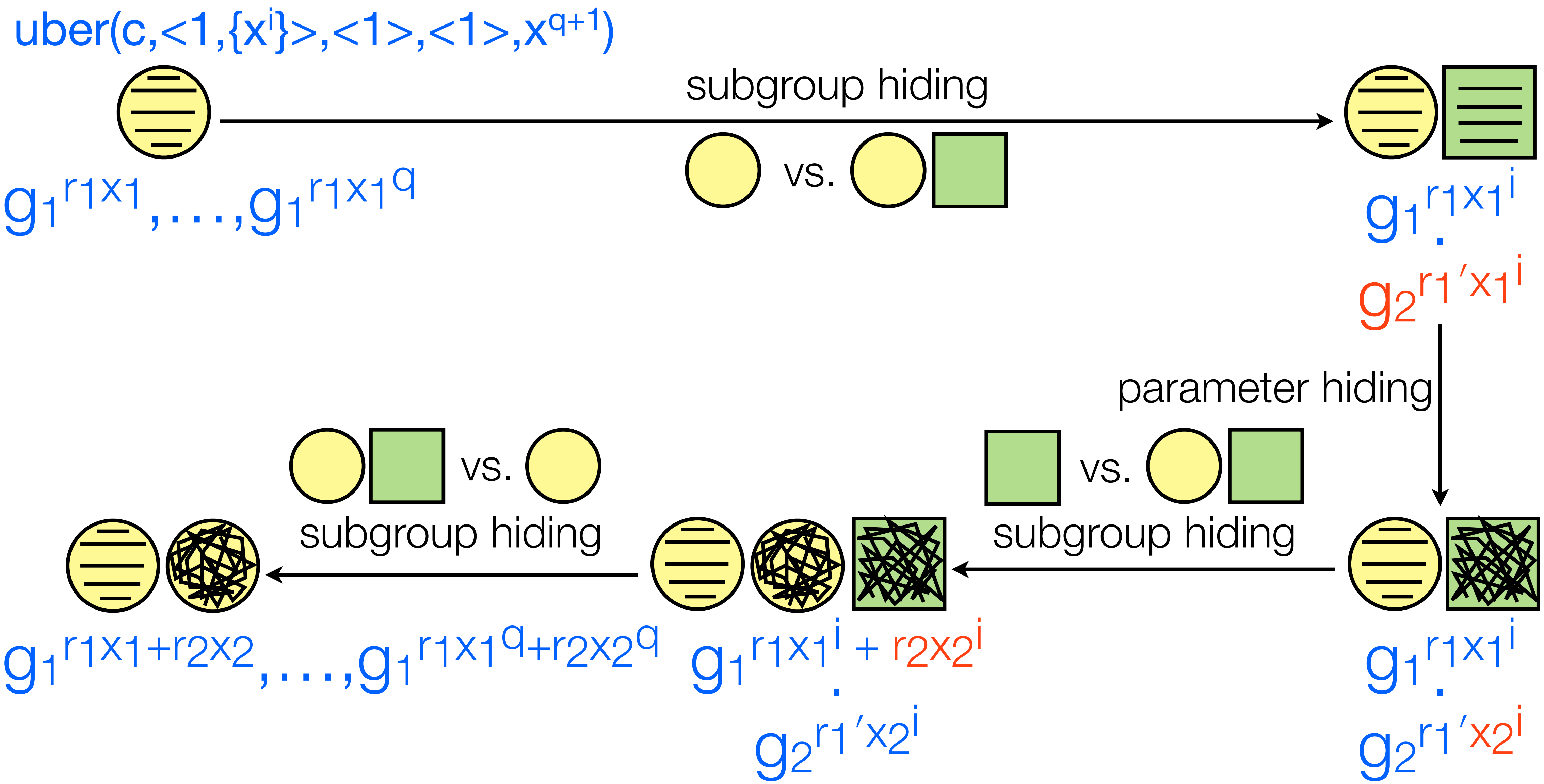
1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to exponent q-SDH



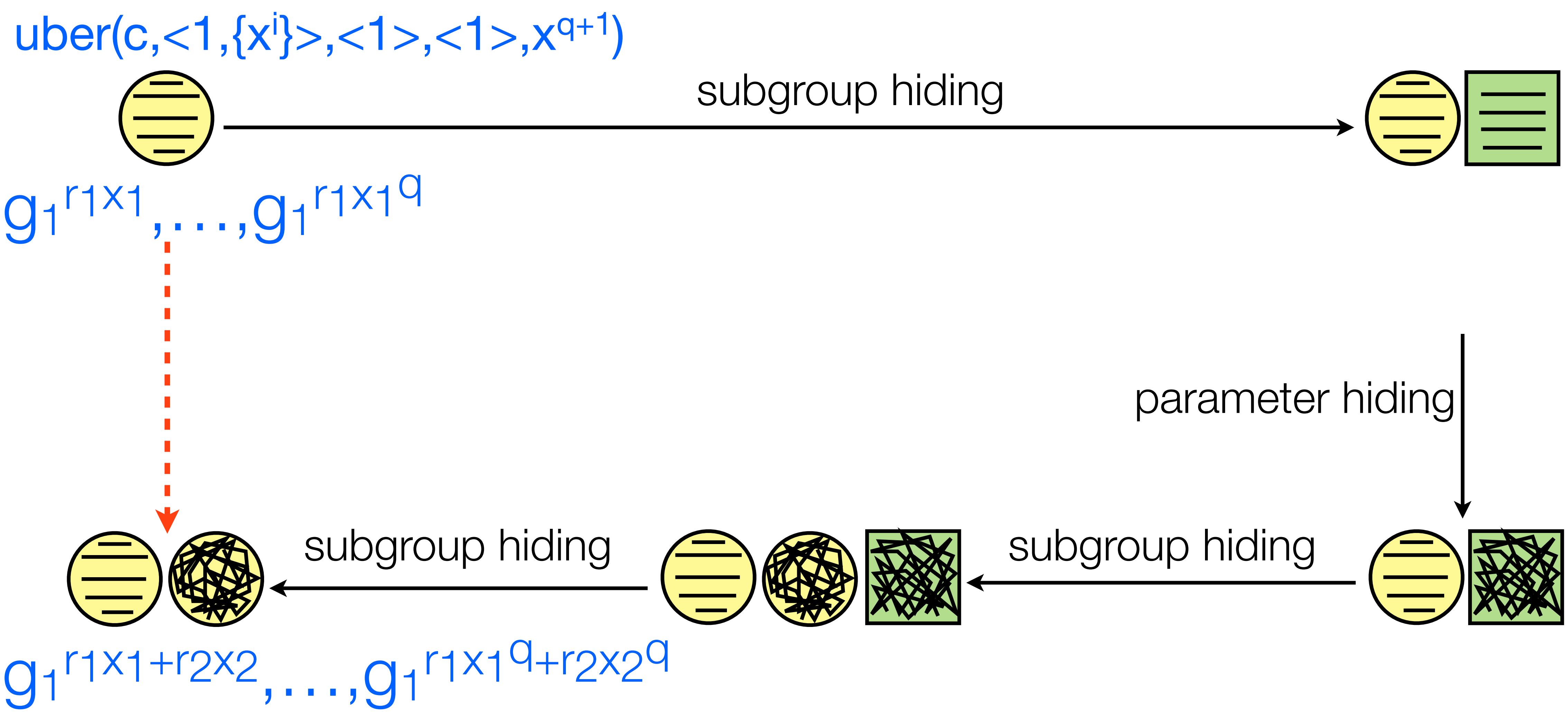
1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to exponent q-SDH



1. start with base scheme
2. transition to SF version
3. argue information is hidden

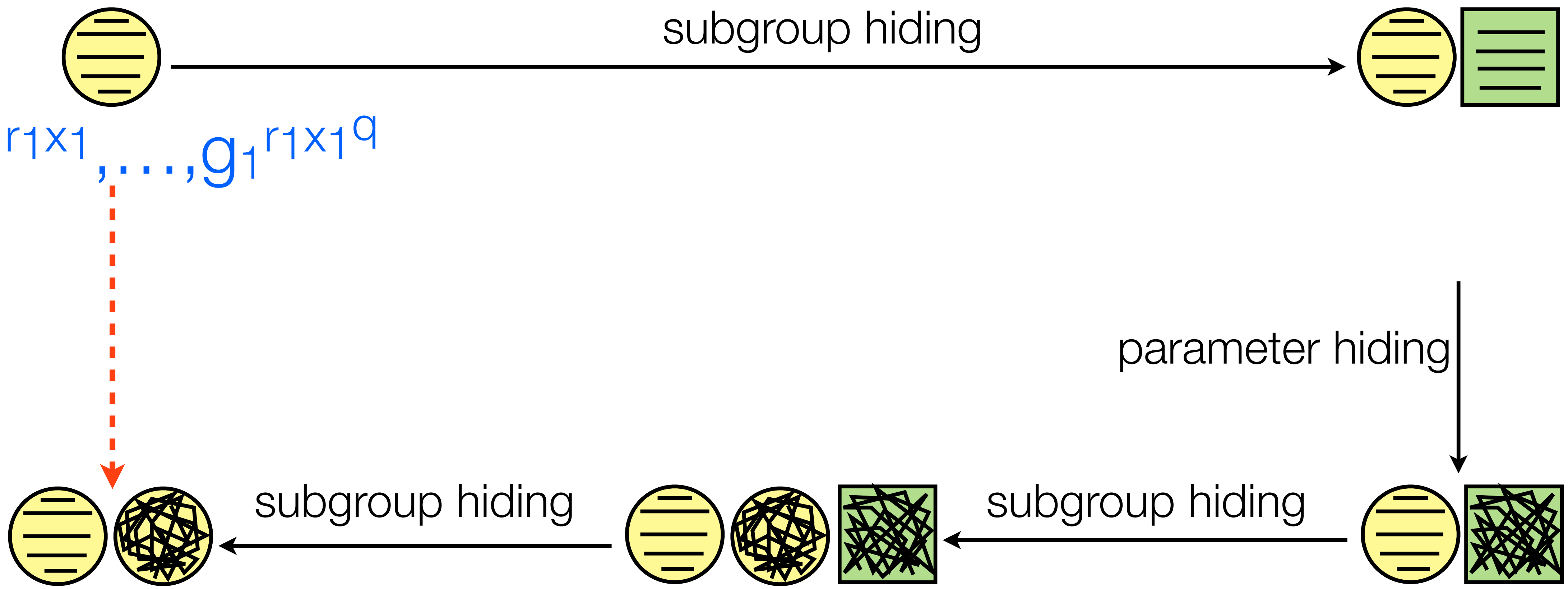
Applying dual systems to exponent q-SDH



1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to exponent q-SDH

$uber(c,<1,\{x^i\}>,<1>,<1>,x^{q+1})$



$g_1^{r_1x_1},\ldots,g_1^{r_1x_1^q}$

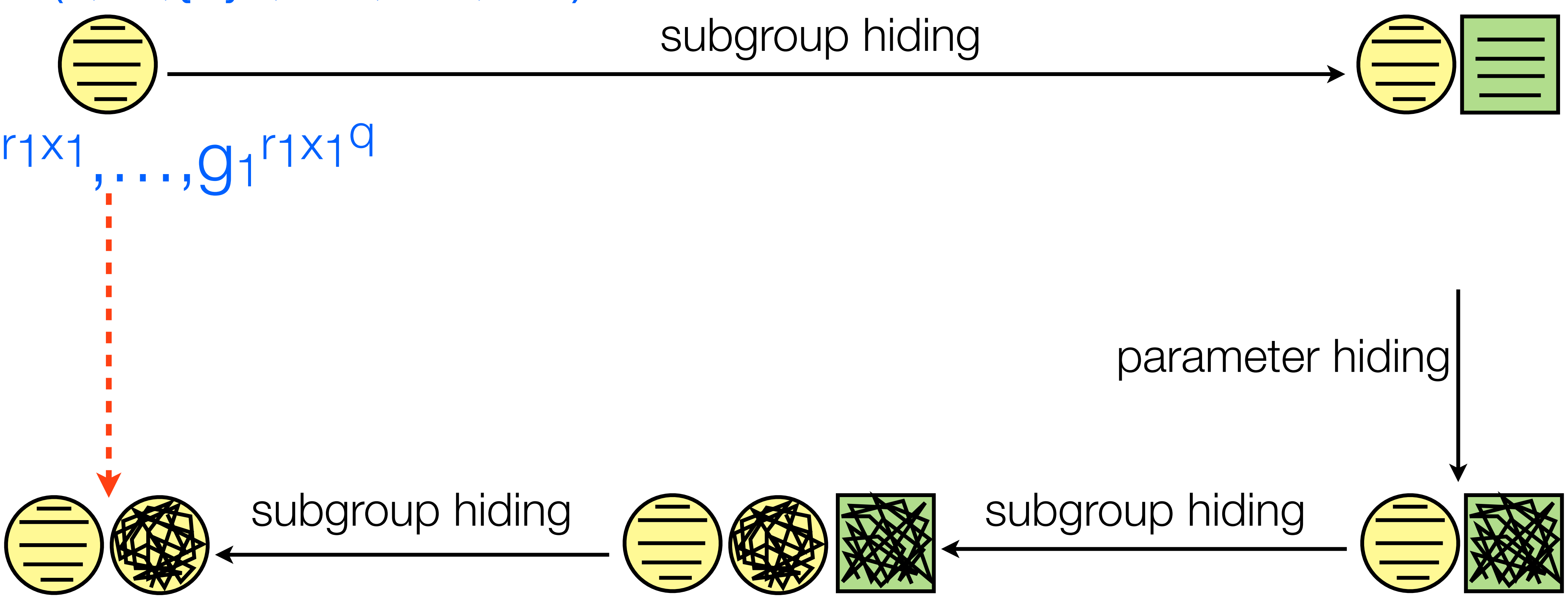
$g_1^{r_1x_1+r_2x_2},\ldots,g_1^{r_1x_1^q+r_2x_2^q}$

$g_1^{\Sigma r_kx_k},\ldots,g_1^{\Sigma r_kx_k^q}$

1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to exponent q-SDH

uber(c,<1,{x^i}>,<1>,<1>,x^{q+1})



$g_1^{r_1 x_1}, \ldots, g_1^{r_1 x_1^q}$

$g_1^{r_1 x_1 + r_2 x_2}, \ldots, g_1^{r_1 x_1^q + r_2 x_2^q}$

$g_1^{\Sigma r_k x_k}, \ldots, g_1^{\Sigma r_k x_k^q}$

1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to exponent q-SDH

1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to exponent q-SDH

$\mathrm{uber}(c,R,\langle 1,\{x^i\}\rangle,\langle 1\rangle,x^{q+1}) \rightarrow \mathrm{uber}(\ell c,\langle 1,\{\sum r_k x_k^i\}\rangle,\langle 1\rangle,\langle 1\rangle,\sum r_k x_k^{q+1})$

1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to exponent q-SDH

$\mathrm{uber}(c,R,\langle 1,\{x^i\}\rangle,\langle 1\rangle,x^{q+1}) \rightarrow \mathrm{uber}(\ell c,\langle 1,\{ \sum r_k x_k^i\}\rangle,\langle 1\rangle,\langle 1\rangle,\sum r_k x_k^{q+1})$

$$\begin{bmatrix} r & r & \dots & r \end{bmatrix} \begin{bmatrix} 1 & x & . & x & x \\ 1 & x & . & x & x \\ . & & . & & . \\ . & & & . & . \\ 1 & x & . & x & x \end{bmatrix}$$

1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to exponent q-SDH

$\mathrm{uber}(c,R,\langle 1,\{x^i\}\rangle,\langle 1\rangle,x^{q+1}) \rightarrow \mathrm{uber}(\ell c,\langle 1,\{\sum r_k x_k^i\}\rangle,\langle 1\rangle,\langle 1\rangle,\sum r_k x_k^{q+1})$

$$\begin{bmatrix} r & r & \dots & r \end{bmatrix} \begin{bmatrix} 1 & x & . & x & x \\ 1 & x & . & x & x \\ . & & . & & . \\ . & & & . & . \\ 1 & x & . & x & x \end{bmatrix} = \begin{bmatrix} y \\ y \\ . \\ . \\ y \end{bmatrix}$$

So A is really given

1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to exponent q-SDH

$$\begin{bmatrix} r & r & \dots & r \end{bmatrix} \begin{bmatrix} 1 & x & . & x & x \\ 1 & x & . & x & x \\ . & & . & & . \\ . & & & . & . \\ 1 & x & . & x & x \end{bmatrix} = \begin{bmatrix} y \\ y \\ . \\ . \\ y \end{bmatrix}$$

1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to exponent q-SDH

$$\begin{bmatrix} r & r & \dots & r \end{bmatrix} \begin{bmatrix} 1 & x & . & x & x \\ 1 & x & . & x & x \\ . & & . & & . \\ . & & & . & . \\ 1 & x & . & x & x \end{bmatrix} = \begin{bmatrix} y \\ y \\ . \\ . \\ y \end{bmatrix}$$

Vandermonde matrix,
so if ℓ=q+2 this is invertible

1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to exponent q-SDH

$$\begin{bmatrix} r & r & \cdots & r \end{bmatrix} \begin{bmatrix} 1 & x & . & x & x \\ 1 & x & . & x & x \\ . & & . & & . \\ . & & & . & . \\ 1 & x & . & x & x \end{bmatrix} = \begin{bmatrix} y \\ y \\ . \\ . \\ y \end{bmatrix}$$

Vandermonde matrix,
so if ℓ=q+2 this is invertible

Consider set S of ℓ-sized sets; then **r**,**y**∈S

Matrix multiplication is ~~map~~ permutation M: S → S

1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to exponent q-SDH

$$\begin{bmatrix} r & r & \dots & r \end{bmatrix} \begin{bmatrix} 1 & x & . & x & x \\ 1 & x & . & x & x \\ . & & . & & . \\ . & & & . & . \\ 1 & x & . & x & x \end{bmatrix} = \begin{bmatrix} y \\ y \\ . \\ . \\ y \end{bmatrix}$$

This is chosen uniformly at random from S

Vandermonde matrix, so if ℓ=q+2 this is invertible

Consider set S of ℓ-sized sets; then **r,y**∈S

Matrix multiplication is ~~map~~ permutation M: S → S

1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to exponent q-SDH

$$\begin{bmatrix} r & r & \dots & r \end{bmatrix} \begin{bmatrix} 1 & x & . & x & x \\ 1 & x & . & x & x \\ . & & . & & . \\ . & & & . & . \\ 1 & x & . & x & x \end{bmatrix} = \begin{bmatrix} y \\ y \\ . \\ . \\ y \end{bmatrix}$$

This is chosen uniformly at random from S

Vandermonde matrix, so if ℓ=q+2 this is invertible

This is distributed uniformly random as well!

Consider set S of ℓ-sized sets; then **r,y**∈S

Matrix multiplication is ~~map~~ permutation M: S → S

1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to the uber-assumption

More generally, this is true if

$$\begin{bmatrix} 1 & \rho & & . & \rho & & f(x & \\ 1 & \rho & & . & \rho & & f(x & \\ . & & . & . & & & & . \\ . & & . & & & . & & . \\ 1 & \rho & & . & \rho & & f(x & \end{bmatrix}$$

has linearly independent columns (or rows)

1. start with base scheme
2. transition to SF version
3. argue information is hidden

Applying dual systems to the uber-assumption

More generally, this is true if

$$\begin{bmatrix} 1 & \rho & & . & \rho & & f(x \\ 1 & \rho & & . & \rho & & f(x \\ . & & . & . & & & . \\ . & & . & & . & & . \end{bmatrix}$$

has li

Decisional uber(c,R,S,T,f) holds if:

1. subgroup hiding and parameter hiding hold

2. S = T = <1>

3. f is not a linear combination of ρ_i

e

n

3. argue information is hidden

Applying dual systems to the uber-assumption

More generally, this is true if

$$\begin{bmatrix} 1 & \rho & . & \rho & f(x \\ 1 & \rho & . & \rho & f(x \\ . & . & . & & . \\ . & . & & . & . \end{bmatrix}$$

only computational requirement

has li

Decisional uber(c,R,S,T,f) holds if:

1. subgroup hiding and parameter hiding hold

2. S = T = <1>

3. f is not a linear combination of ρ_i

3. argue information is hidden

Applying dual systems to the uber-assumption

More generally, this is true if

$$\begin{bmatrix} 1 & \rho & & . & \rho & & f(x & \\ 1 & \rho & & . & \rho & & f(x & \\ . & & . & . & & & & . \\ . & & . & & & . & & . \end{bmatrix}$$

only computational requirement

has li

Decisional uber(c,R,S,T,f) holds if:

1. subgroup hiding and parameter hiding hold

limitation → 2. $S = T = \langle 1 \rangle$

3. f is not a linear combination of ρ_i

3. argue information is hidden

Outline

Bilinear groups

q-Type assumptions

Extensions

Broader classes of assumptions

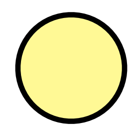
Dodis-Yampolskiy PRF

Conclusions

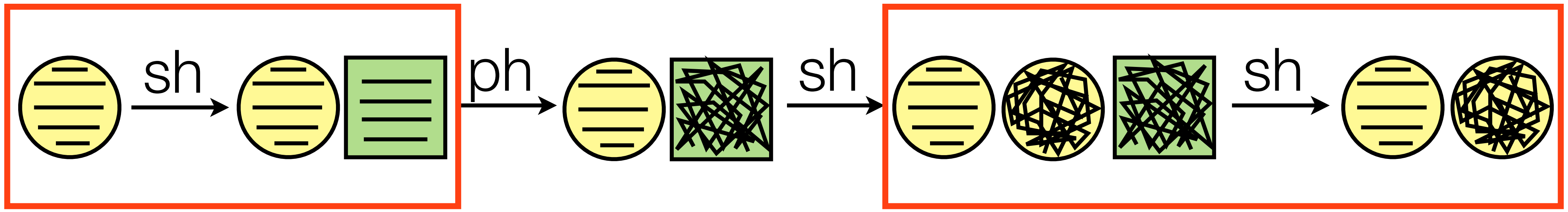
Strengthening our results

Strengthening our results

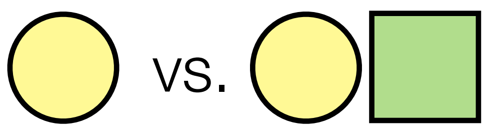
Remember that we needed two types of subgroup hiding …

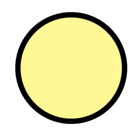
…even when given a generator for 

Strengthening our results

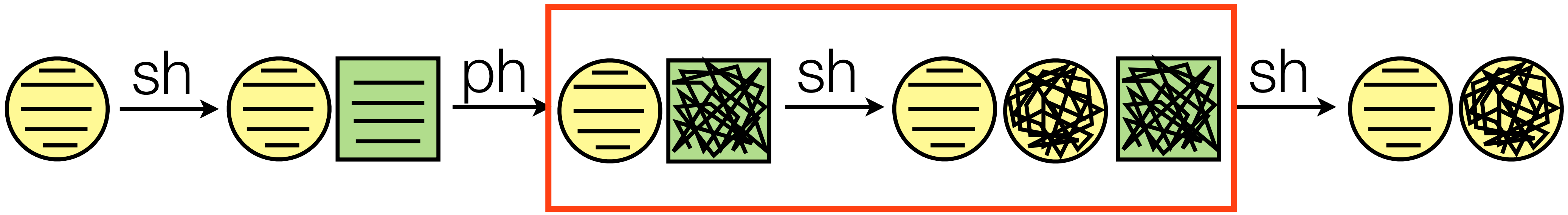


Remember that we needed two types of subgroup hiding …

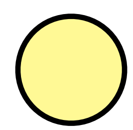


…even when given a generator for 

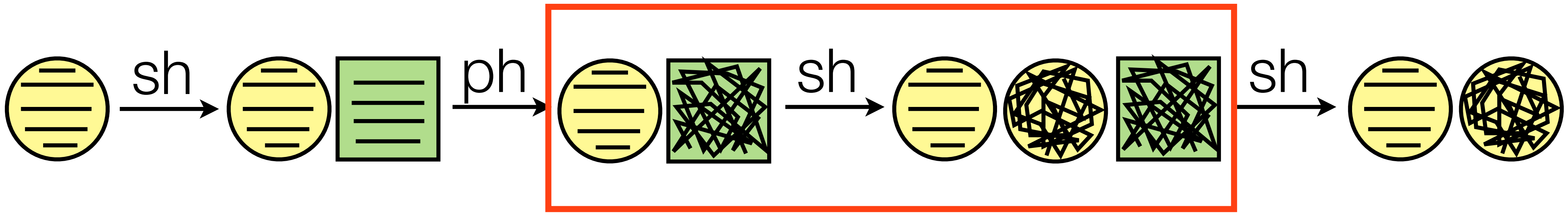
Strengthening our results



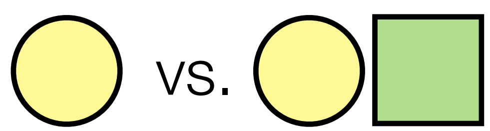
Remember that we needed two types of subgroup hiding …

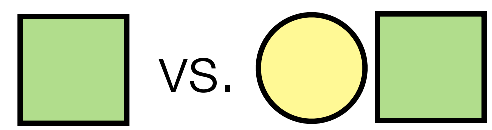
…even when given a generator for 

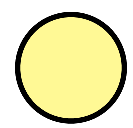
Strengthening our results



Remember that we needed two types of subgroup hiding …



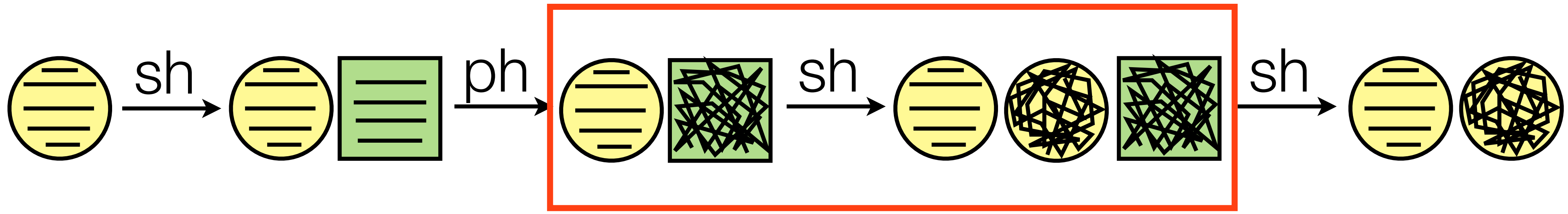


…even when given a generator for 

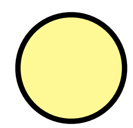
This restricts us to “one-sided” assumptions

2. S = T = <1>

Strengthening our results



Remember that we needed two types of subgroup hiding …

…even when given a generator for 

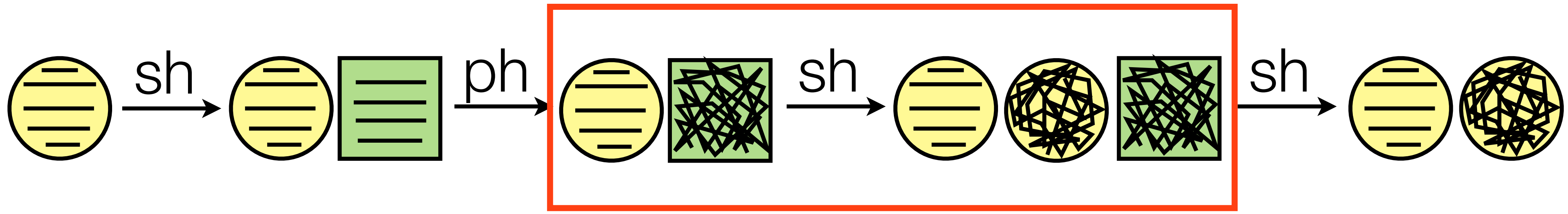
This restricts us to “one-sided” assumptions

2. S = T = <1>

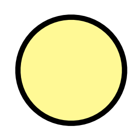
[eq-SDH]

$$(g, g^{x}, \ldots, g^{x^{q}}) \rightarrow g^{x^{q+1}} \text{ or random}$$

Strengthening our results



Remember that we needed two types of subgroup hiding …

…even when given a generator for 

This restricts us to "one-sided" assumptions

2. S = T = <1>

[eq-SDH] $(g,g^x,\ldots,g^{x^q}) \rightarrow g^{x^{q+1}}$ or random

[q-SDH] $(g,g^x,\ldots,g^{x^q},h^x) \rightarrow$ compute $(c,g^{1/x+c})$

Strengthening our results

Remember that we needed two types of subgroup hiding…

Strengthening our results

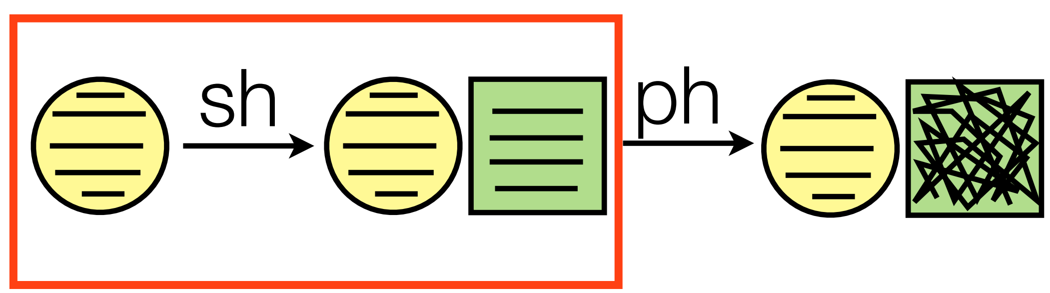
Remember that we needed two types of subgroup hiding…

To address this, switch back to regular dual systems

Strengthening our results

Remember that we needed two types of subgroup hiding…

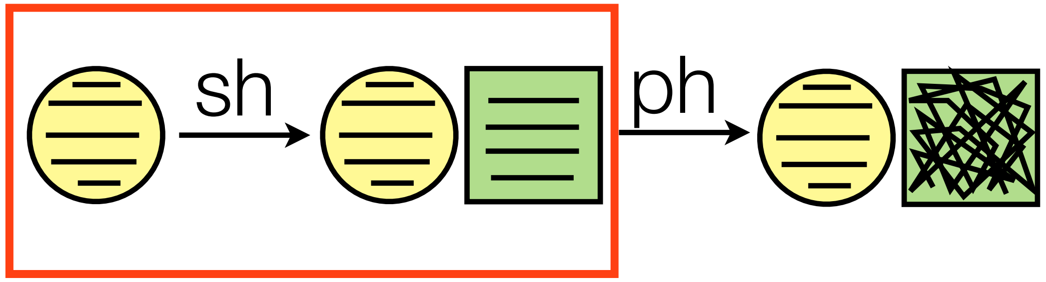
To address this, switch back to regular dual systems



Strengthening our results

Remember that we needed two types of subgroup hiding…

To address this, switch back to regular dual systems



Strengthening our results

Remember that we needed two types of subgroup hiding…

To address this, switch back to regular dual systems

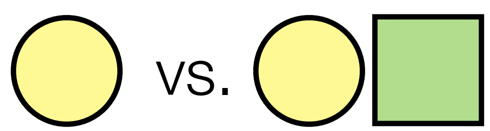
limitation

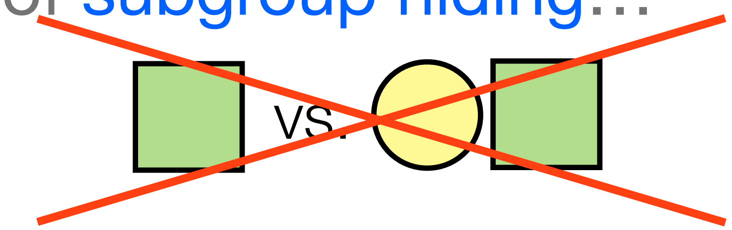
Computational uber(c,R,S,T,f) holds if:

1. subgroup hiding and parameter hiding hold
2. f is not a linear combination of ρ_i

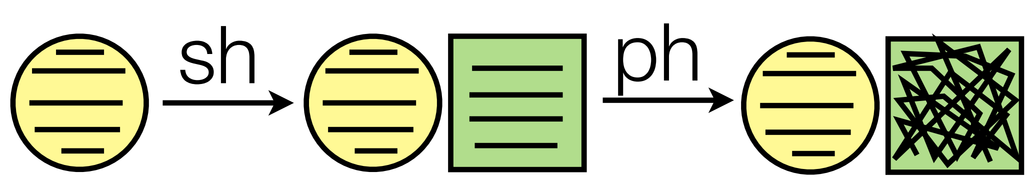
Strengthening our results

Remember that we needed two types of subgroup hiding…





To address this, switch back to regular dual systems



This implies (for example) that q-SDH [BB04] follows from subgroup hiding....

…and so does everything based on q-SDH (like Boneh-Boyen signatures)*

*when instantiated in asymmetric composite-order groups [BRS11]

Reexamining the Dodis-Yampolskiy PRF

$f(x) = u^{1/sk+x}$ for fixed $sk \leftarrow \mathcal{R}$; $x \in a(\lambda)$

Reexamining the Dodis-Yampolskiy PRF

$f(x) = u^{1/sk+x}$ for fixed $sk \leftarrow \mathcal{R}$; $x \in a(\lambda)$

Theorem [DY05]: $\mathrm{Adv}^{\mathrm{vrf}} \leq a(\lambda) \cdot \mathrm{Adv}^{a(\lambda)\text{-DBDHI}}$

Reexamining the Dodis-Yampolskiy PRF

$f(x) = u^{1/sk+x}$ for fixed $sk \leftarrow \mathcal{R}$; $x \in a(\lambda)$

Theorem [DY05]: $\mathrm{Adv}^{\boxed{\mathrm{vrf}}} \leq a(\lambda) \cdot \mathrm{Adv}^{a(\lambda)\text{-DBDHI}}$

verifiable random function

Reexamining the Dodis-Yampolskiy PRF

$f(x) = \boxed{u}^{1/sk+x}$ for fixed $sk \leftarrow \mathcal{R}$; $x \in a(\lambda)$

Theorem [DY05]: $Adv^{\boxed{vrf}} \le a(\lambda) \cdot Adv^{a(\lambda)\text{-DBDHI}}$

- verifiable random function
- require $u=e(g,h)$

Reexamining the Dodis-Yampolskiy PRF

$f(x) = \boxed{u}^{1/sk+x}$ for fixed $sk \leftarrow \mathcal{R}$; $x \in a(\lambda)$

Theorem [DY05]: $\mathrm{Adv}^{\boxed{\mathrm{vrf}}} \leq a(\lambda) \cdot \mathrm{Adv}^{\boxed{a(\lambda)\text{-DBDHI}}}$

- verifiable random function
- q-type assumption
- require $u = e(g,h)$

Reexamining the Dodis-Yampolskiy PRF

$f(x) = \boxed{u}^{1/sk+x}$ for fixed $sk \leftarrow \mathcal{R}$; $x \in a(\lambda)$

Theorem [DY05]: $\mathrm{Adv}^{\boxed{\mathrm{vrf}}} \leq \boxed{a(\lambda)} \cdot \mathrm{Adv}^{\boxed{a(\lambda)\text{-DBDHI}}}$

- verifiable random function
- require $u=e(g,h)$
- q-type assumption
- looseness: need $|a(\lambda)| \leq \mathrm{poly}(\lambda)$

Reexamining the Dodis-Yampolskiy PRF

$f(x) = u^{1/sk+x}$ for fixed $sk \leftarrow \mathcal{R}$; $x \in a(\lambda)$

Theorem [DY05]: $\mathrm{Adv}^{vrf} \leq a(\lambda) \cdot \mathrm{Adv}^{a(\lambda)\text{-DBDHI}}$

- verifiable random function
- require $u=e(g,h)$
- q-type assumption
- looseness: need $|a(\lambda)| \leq \mathrm{poly}(\lambda)$

Theorem: $\mathrm{Adv}^{prf} \leq q \cdot \mathrm{Adv}^{sgh}$

Reexamining the Dodis-Yampolskiy PRF

$f(x) = u^{1/sk+x}$ for fixed $sk \leftarrow \mathcal{R}$; $x \in a(\lambda)$

Theorem [DY05]: $\mathrm{Adv}^{vrf} \leq a(\lambda) \cdot \mathrm{Adv}^{a(\lambda)\text{-DBDHI}}$

- verifiable random function
- require $u = e(g,h)$
- q-type assumption
- looseness: need $|a(\lambda)| \leq \mathrm{poly}(\lambda)$

Theorem: $\mathrm{Adv}^{\boxed{prf}} \leq q \cdot \mathrm{Adv}^{sgh}$

- pseudorandom function

Reexamining the Dodis-Yampolskiy PRF

$f(x) = \boxed{u}^{1/sk+x}$ for fixed $sk \leftarrow \mathcal{R}$; $x \in a(\lambda)$

Theorem [DY05]: $\mathrm{Adv}^{vrf} \leq a(\lambda) \cdot \mathrm{Adv}^{a(\lambda)\text{-DBDHI}}$

- verifiable random function
- require $u=e(g,h)$
- q-type assumption
- looseness: need $|a(\lambda)| \leq poly(\lambda)$

Theorem: $\mathrm{Adv}^{\boxed{prf}} \leq q \cdot \mathrm{Adv}^{sgh}$

- pseudorandom function
- require composite order

Reexamining the Dodis-Yampolskiy PRF

$f(x) = \boxed{u}^{1/sk+x}$ for fixed $sk \leftarrow \mathcal{R}$; $x \in a(\lambda)$

Theorem [DY05]: $\mathrm{Adv}^{\mathrm{vrf}} \leq a(\lambda) \cdot \mathrm{Adv}^{a(\lambda)\text{-DBDHI}}$

- verifiable random function
- require $u=e(g,h)$
- q-type assumption
- looseness: need $|a(\lambda)| \leq \mathrm{poly}(\lambda)$

Theorem: $\mathrm{Adv}^{\boxed{\mathrm{prf}}} \leq q \cdot \mathrm{Adv}^{\boxed{\mathrm{sgh}}}$

- pseudorandom function
- require composite order
- static assumption

Reexamining the Dodis-Yampolskiy PRF

$f(x) = \boxed{u}^{1/sk+x}$ for fixed $sk \leftarrow \mathcal{R}$; $x \in a(\lambda)$

Theorem [DY05]: $\mathrm{Adv}^{\mathrm{vrf}} \le a(\lambda) \cdot \mathrm{Adv}^{a(\lambda)\text{-DBDHI}}$

- verifiable random function
- require u=e(g,h)
- q-type assumption
- looseness: need $|a(\lambda)| \le \mathrm{poly}(\lambda)$

Theorem: $\mathrm{Adv}^{\boxed{\mathrm{prf}}} \le \boxed{q} \cdot \mathrm{Adv}^{\boxed{\mathrm{sgh}}}$

- pseudorandom function
- require composite order
- static assumption
- $a(\lambda)$ of arbitrary size

Outline

Bilinear groups	q-Type assumptions
Extensions	Conclusions

Conclusions and open problems

Conclusions and open problems

We applied the dual-system technique directly to a broad class of assumptions

Conclusions and open problems

We applied the dual-system technique directly to a broad class of assumptions

Limitation: Restricted to (asymmetric) composite-order (bilinear) groups

Conclusions and open problems

We applied the dual-system technique directly to a broad class of assumptions

Limitation: Restricted to (asymmetric) composite-order (bilinear) groups

Limitation: Can’t get rid of every q-type assumption

Conclusions and open problems

We applied the dual-system technique directly to a broad class of assumptions

Limitation: Restricted to (asymmetric) composite-order (bilinear) groups

Limitation: Can't get rid of every q-type assumption

Full version!: `cs.ucsd.edu/~smeiklejohn/files/eurocrypt14a.pdf`

Conclusions and open problems

We applied the dual-system technique directly to a broad class of assumptions

Limitation: Restricted to (asymmetric) composite-order (bilinear) groups

Limitation: Can't get rid of every q-type assumption

Full version!: `cs.ucsd.edu/~smeiklejohn/files/eurocrypt14a.pdf`

Thanks! Any questions?