# Déjà Q All Over Again: Tighter and Broader Reductions of $q$-Type Assumptions

Melissa Chase - MSR Redmond
Mary Maller - University College London
Sarah Meiklejohn - University College London

Multilinear Maps | Quadratic Residues | PPAD

Phi Hiding | Ring LWE | Subgroup Hiding | Gap

LWE | Factoring

Shortest Vector | RSA

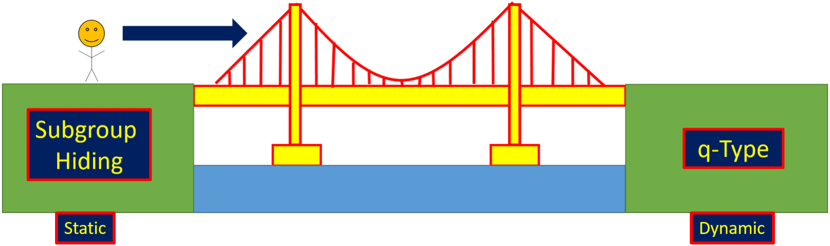
Closest Vector | Discrete Log

Isogenies | Bilinear Diffie Hellman

Code Based | One Way Functions | q-Type | ACD

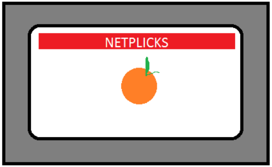
Probabilistic iO | Random Oracles | Generic Group | LPN

UCE | Knowledge Extractors | Obfuscation




*Subgroup Hiding* $\Rightarrow$ *certain q-Type Assumptions*

# Example: Broadcast Encryption




Methods of delivering encrypted content over a broadcast channel where only qualified users can decrypt the content.

## Example

*Boneh Gentry and Waters' broadcast encryption scheme [BGW-Crypto05].*

- *Pairing based solution*
- *Short ciphertexts and private keys*
- *Collusion resistant*

# The $q$-BDHE Assumption

The BGW broadcast encryption scheme bases its security on the $q$-BDHE assumption [BGW-Crypto05].

*Given*

$$g, g^c, g^\alpha, \ldots, g^{\alpha^q}, g^{\alpha^{q+2}}, \ldots, g^{\alpha^{2q}}$$

*it is hard to distinguish* $e(g, g^c)^{q+1}$ *from random.*

# The $q$-BDHE Assumption

The BGW broadcast encryption scheme bases its security on the $q$-BDHE assumption [BGW-Crypto05].

*Given*

$$g, g^c, g^{\alpha}, \ldots, g^{\alpha^q}, ?, g^{\alpha^{q+2}}, \ldots, g^{\alpha^{2q}}$$

*it is hard to distinguish* $e(g, g^c)^{q+1}$ *from random.*

# Déjà Q: Using Dual Systems to Revisit $q$-Type Assumptions [CM-Eurocrypt14]

| | | |
|---|---|---|
| Subgroup Hiding<br>&<br>Parameter Hiding | $\Rightarrow$ | Specific classes of $q$-type assumptions in asymmetric bilinear groups of order $N = p_1 p_2$[1]. |

$$\Pr[\text{break } q\text{-type assumption}] \leq \mathcal{O}(q) \Pr[\text{break subgroup hiding}]$$

[1] Asymmetric composite order bilinear groups do exist - see [BRS-JNT11].

# [CM-Eurocrypt14]: Contributions

| | Decides | Computes |
|---|---|---|
| **Source Group** | | |
| given info in one group | 🙂 | 🙂 |
| given info in both groups | 🙁 | 🙂 |
| **Target Group** | | |
| given info in one group | 🙂 | 🙂 |
| given info in both groups | 🙁 $q$-BDHE | 🙁 |

# Our Contributions: Broader

| | Decides | Computes |
|---|---|---|
| **Source Group** | | |
| given info in one group |  |  |
| given info in both groups |  |  |
| **Target Group** | | |
| given info in one group |  |  |
| given info in both groups |  $q$-BDHE |  |

# Our Contributions: Tighter

Subgroup Hiding & Parameter Hiding $\Rightarrow$ Specific classes of $q$-type assumptions in asymmetric bilinear groups of order $N = p_1 p_2 p_3$.

$$\Pr[\text{break } q\text{-type assumption}] \leq \mathcal{O}(\log q) \Pr[\text{break subgroup hiding}]$$

# Outline of Presentation

Bilinear Groups and Assumptions

Tight Reduction

Symmetric Schemes

Conclusion

# Bilinear Groups

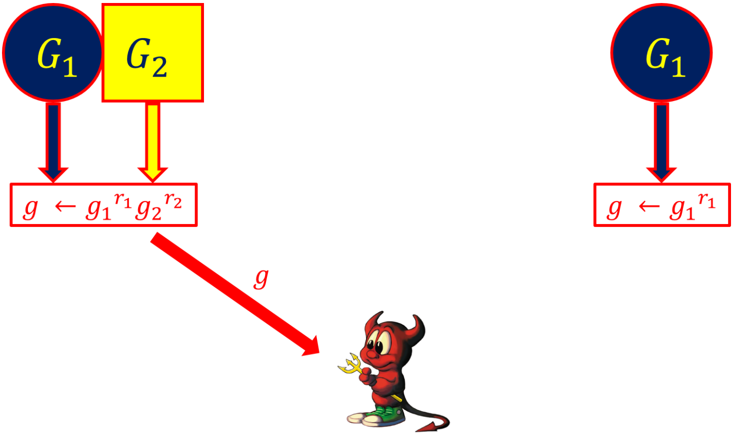
Standard Bilinear Groups: $\mathcal{G} = (N, \mathbb{G}, \mathbb{H}, \mathbb{G}_T, e, g, h)$.

- $N$ = group order; prime or composite
- $|\mathbb{G}| = |\mathbb{H}| = kN$, $|\mathbb{G}_T| = \lambda N$
- $\mathbb{G} =< g >$, $\mathbb{H} =< h >$
- $e : \mathbb{G} \times \mathbb{H} \to \mathbb{G}_T$

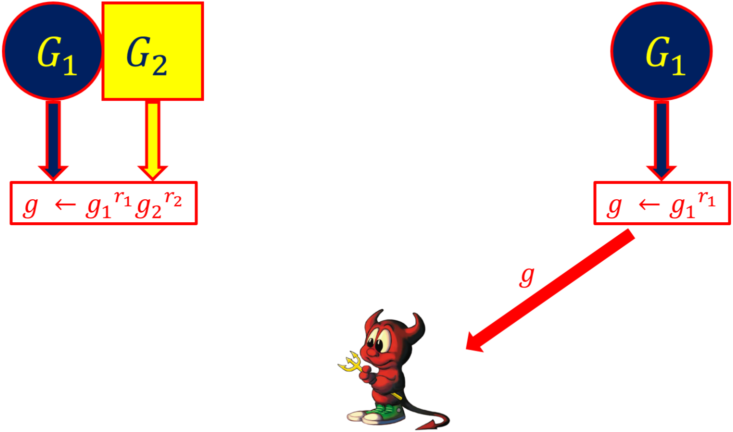
## Properties

*Bilinearity:* $e(g^a, h^b) = e(g, h)^{ab}$
*Non-degeneracy:* $e(x, y) = 1 \forall y \in \mathbb{H} \Rightarrow x = 1.$

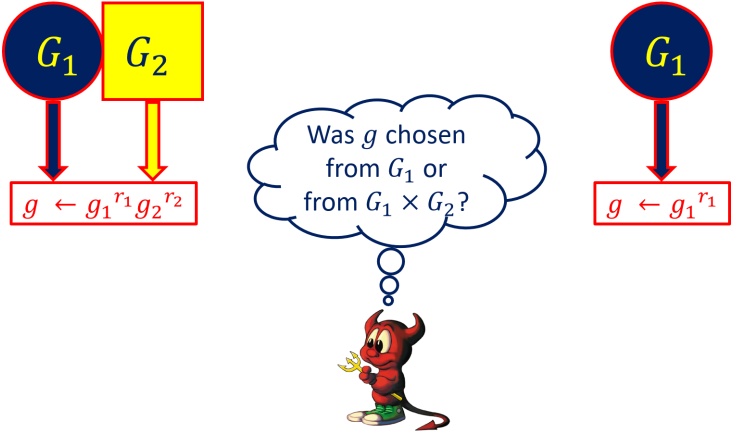
# Subgroup Hiding [BGN - TCC05]



# Subgroup Hiding [BGN - TCC05]



# Subgroup Hiding [BGN - TCC05]



# Parameter Hiding [Lewko-Eurocrypt12]

$G_1$ $G_2$

$g \leftarrow (g_1 g_2)^{rf(x)}$

$r \leftarrow \mathbb{Z}_N$

$f(X) \leftarrow \mathbb{Z}_N[X]$

$x \leftarrow \mathbb{Z}_N$

$g$

$G_1$ $G_2$

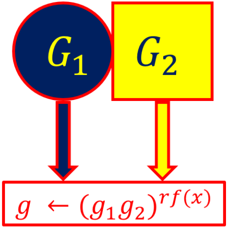
$g \leftarrow {g_1}^{rf(x)} {g_2}^{sf(y)}$

$r, s \leftarrow \mathbb{Z}_N$

$f(X) \leftarrow \mathbb{Z}_N[X]$

$x, y \leftarrow \mathbb{Z}_N$

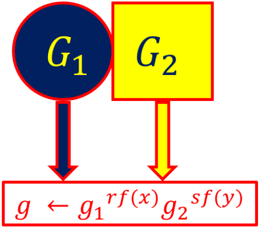
# Parameter Hiding [Lewko-Eurocrypt12]




$r \leftarrow \mathbb{Z}_N$

$f(X) \leftarrow \mathbb{Z}_N[X]$

$x \leftarrow \mathbb{Z}_N$



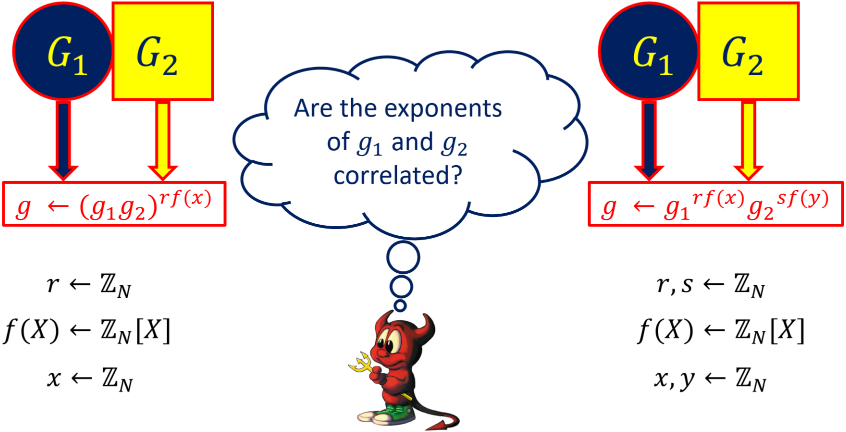

$g$

$r, s \leftarrow \mathbb{Z}_N$

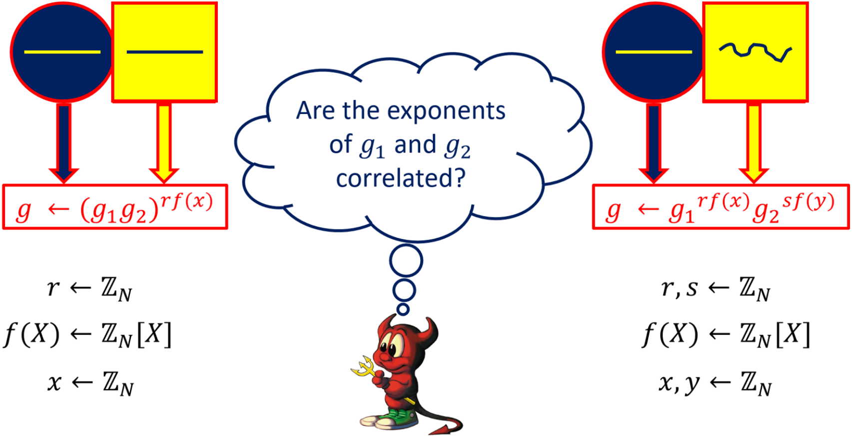
$f(X) \leftarrow \mathbb{Z}_N[X]$

$x, y \leftarrow \mathbb{Z}_N$

# Parameter Hiding [Lewko-Eurocrypt12]



# Parameter Hiding [Lewko-Eurocrypt12]



# Outline of Presentation

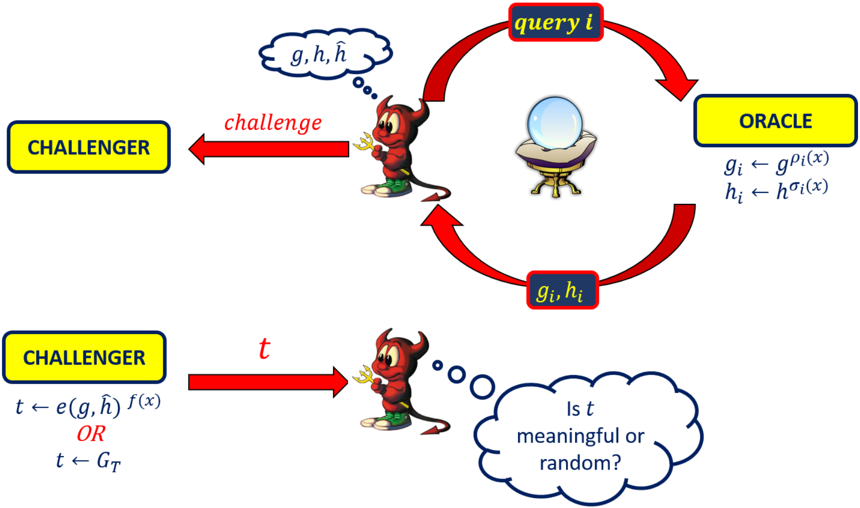
Bilinear Groups and Assumptions

Tight Reduction

Symmetric Schemes

Conclusion

# Reductions we can Cover



# Aim of Reduction

Model $q$-type assumption as a game. Transition to statistically impossible game. [CM-Eurocrypt14]

$$(g_1g_2g_3)^{\rho_1(x)}, \dots, (g_1g_2g_3)^{\rho_q(x)} \in G_1 \times G_2 \times G_3$$

$$(h_1h_2h_3)^{\sigma_1(x)}, \dots, (h_1h_2h_3)^{\sigma_q(x)} \in H_1 \times H_2 \times H_3$$

$$\hat{h} \in H_1 \times H_2 \times H_3$$

$$y = e(g_1g_2g_3, \hat{h})^{f(x)} \in G_T$$

Meaningful

$$(g_1g_2g_3)^{\rho_1(x)}, \dots, (g_1g_2g_3)^{\rho_q(x)} \in G_1 \times G_2 \times G_3$$

$$(h_1h_2h_3)^{\sigma_1(x)}, \dots, (h_1h_2h_3)^{\sigma_q(x)} \in H_1 \times H_2 \times H_3$$

$$\hat{h} \in H_1 \times H_2 \times H_3$$

$$y \xleftarrow{r} G_T$$

# Aim of Reduction

Model $q$-type assumption as a game. Transition to statistically impossible game. [CM-Eurocrypt14]

$\boxed{(g_1g_2g_3)^{\rho_1(x)}, \dots, (g_1g_2g_3)^{\rho_q(x)} \in G_1 \times G_2 \times G_3}$

$\boxed{(h_1h_2h_3)^{\sigma_1(x)}, \dots, (h_1h_2h_3)^{\sigma_q(x)} \in H_1 \times H_2 \times H_3}$

$\boxed{\hat{h} \in H_1 \times H_2 \times H_3}$

$\boxed{y = e(g_1g_2g_3, \hat{h})^{f(x)} \in G_T}$

$\boxed{(g_1g_2g_3)^{\rho_1(x)}, \dots, (g_1g_2g_3)^{\rho_q(x)} \in G_1 \times G_2 \times G_3}$

$\boxed{(h_1h_2h_3)^{\sigma_1(x)}, \dots, (h_1h_2h_3)^{\sigma_q(x)} \in H_1 \times H_2 \times H_3}$

$\boxed{\hat{h} \in H_1 \times H_2 \times H_3}$

$\boxed{y \xleftarrow{r} G_T}$

Random

# Aim of Reduction

Model $q$-type assumption as a game. Transition to statistically impossible game. [CM-Eurocrypt14]

$$(g_1 g_2 g_3)^{\rho_1(x)}, \dots, (g_1 g_2 g_3)^{\rho_q(x)} \in G_1 \times G_2 \times G_3$$
$$(h_1 h_2 h_3)^{\sigma_1(x)}, \dots, (h_1 h_2 h_3)^{\sigma_q(x)} \in H_1 \times H_2 \times H_3$$
$$\hat{h} \in H_1 \times H_2 \times H_3$$
$$y = e(g_1 g_2 g_3, \hat{h})^{f(x)} \in G_T$$

$$(g_1 g_2 g_3)^{\rho_1(x)}, \dots, (g_1 g_2 g_3)^{\rho_q(x)} \in G_1 \times G_2 \times G_3$$
$$(h_1 h_2 h_3)^{\sigma_1(x)}, \dots, (h_1 h_2 h_3)^{\sigma_q(x)} \in H_1 \times H_2 \times H_3$$
$$\hat{h} \in H_1 \times H_2 \times H_3$$
$$y \stackrel{r}{\leftarrow} G_T$$

# Aim of Reduction

Model $q$-type assumption as a game. Transition to statistically impossible game. [CM-Eurocrypt14]

$\boxed{g_1{}^{\rho_1(x)} g_2{}^{r_1}, \ldots, g_1{}^{\rho_q(x)} g_2{}^{r_q} \in G_1 \times G_2}$

$\boxed{h_1{}^{\sigma_1(x)}, \ldots, h_1{}^{\sigma_q(x)} \in H_1}$

$\boxed{\hat{h} \in H_1 \times H_2 \times H_3}$

$\boxed{y = e(g_1{}^{f(x)} g_2{}^{r}, \hat{h}) \ \in G_T}$

Random

$\boxed{g_1{}^{\rho_1(x)} g_2{}^{r_1}, \ldots, g_1{}^{\rho_q(x)} g_2{}^{r_q} \in G_1 \times G_2}$

$\boxed{h_1{}^{\sigma_1(x)}, \ldots, h_1{}^{\sigma_q(x)} \in H_1}$

$\boxed{\hat{h} \in H_1 \times H_2 \times H_3}$

$\boxed{y \xleftarrow{r} G_T}$

# Aim of Reduction

Model $q$-type assumption as a game. Transition to statistically impossible game. [CM-Eurocrypt14]

$\boxed{{g_1}^{\rho_1(x)}{g_2}^{r_1},\dots,{g_1}^{\rho_q(x)}{g_2}^{r_q} \in G_1 \times G_2}$

$\boxed{{h_1}^{\sigma_1(x)},\dots,{h_1}^{\sigma_q(x)} \in H_1}$

$\boxed{\hat{h} \in H_1 \times H_2 \times H_3}$

$\boxed{y = e({g_1}^{f(x)}{g_2}^{r},\hat{h}) \ \in G_T}$

$\boxed{{g_1}^{\rho_1(x)}{g_2}^{r_1},\dots,{g_1}^{\rho_q(x)}{g_2}^{r_q} \in G_1 \times G_2}$

$\boxed{{h_1}^{\sigma_1(x)},\dots,{h_1}^{\sigma_q(x)} \in H_1}$

$\boxed{\hat{h} \in H_1 \times H_2 \times H_3}$

$\boxed{y \xleftarrow{r} G_T}$

Random

# Aim of Reduction

Model $q$-type assumption as a game. Transition to statistically impossible game. [CM-Eurocrypt14]

$$\boxed{{g_1}^{\rho_1(x)}{g_2}^{r_1}, \dots, {g_1}^{\rho_q(x)}{g_2}^{r_q} \in G_1 \times G_2}$$

$$\boxed{{h_1}^{\sigma_1(x)}, \dots, {h_1}^{\sigma_q(x)} \in H_1}$$

$$\boxed{\hat{h} \in H_1 \times H_2 \times H_3}$$

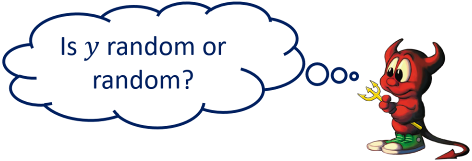
$$\boxed{y = e({g_1}^{f(x)}{g_2}^{r}, \hat{h}) \ \in G_T}$$

$$\boxed{{g_1}^{\rho_1(x)}{g_2}^{r_1}, \dots, {g_1}^{\rho_q(x)}{g_2}^{r_q} \in G_1 \times G_2}$$

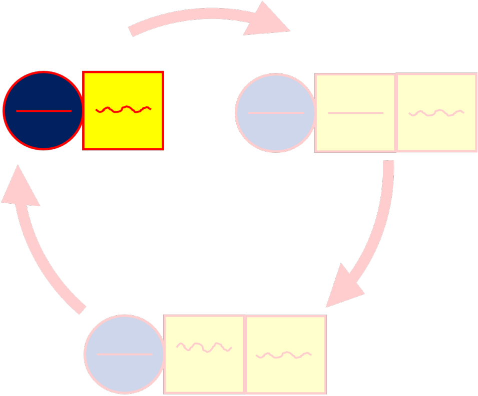
$$\boxed{{h_1}^{\sigma_1(x)}, \dots, {h_1}^{\sigma_q(x)} \in H_1}$$

$$\boxed{\hat{h} \in H_1 \times H_2 \times H_3}$$

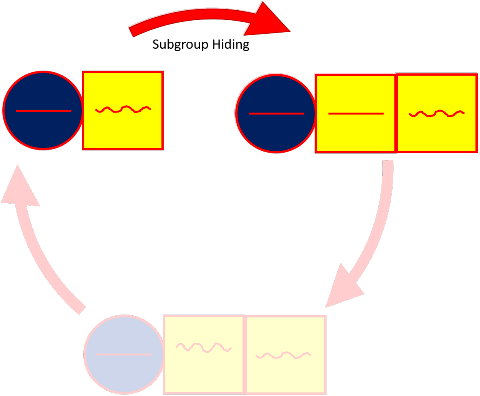
$$\boxed{y \xleftarrow{r} G_T}$$



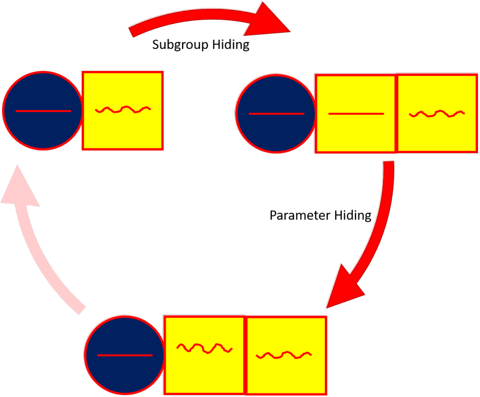
# Déjà Q: Reduction Techniques



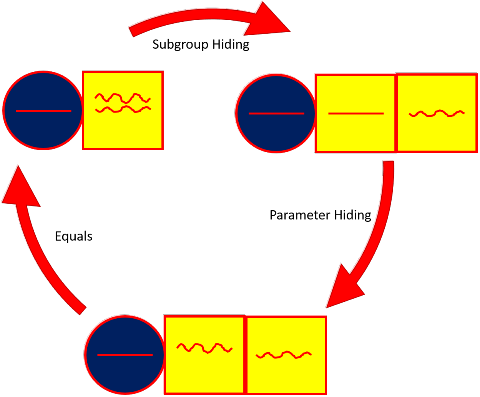
# Déjà Q: Reduction Techniques



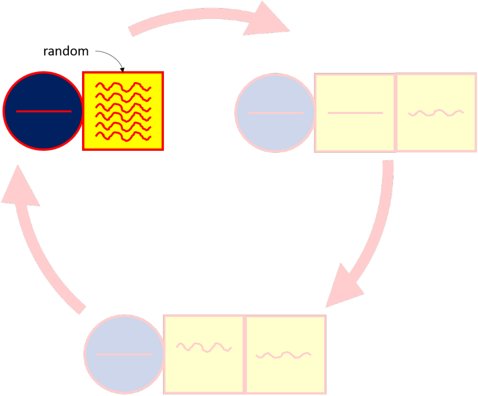
# Déjà Q: Reduction Techniques



# Déjà Q: Reduction Techniques

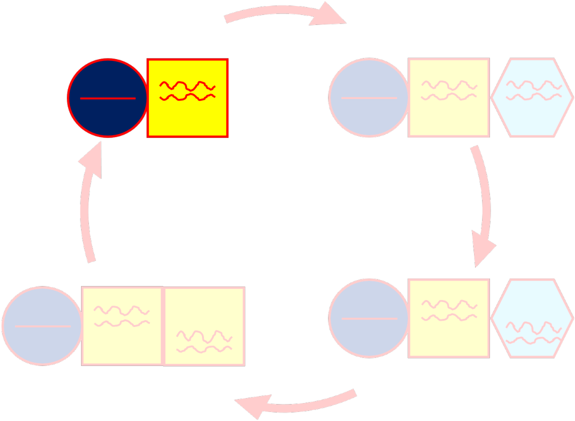


# Déjà Q: Reduction Techniques



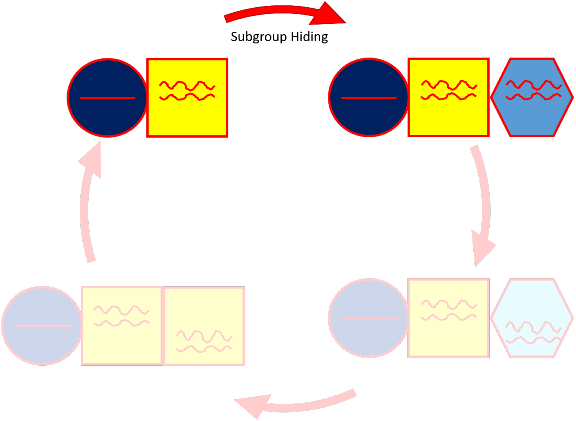
# Our Tight Reduction Techniques

Double the randomness.



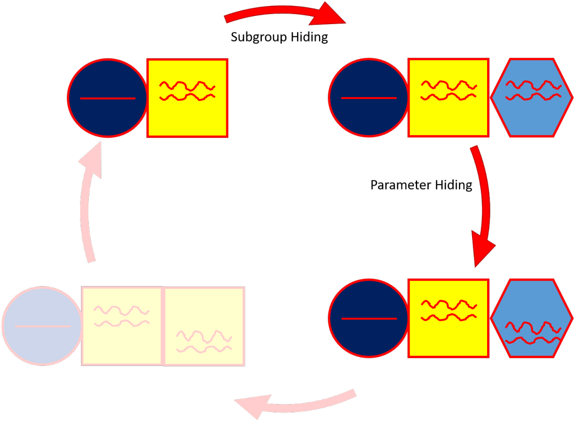
# Our Tight Reduction Techniques

Double the randomness.



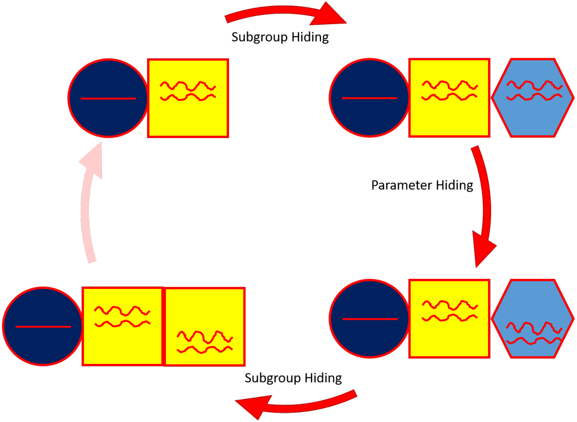
# Our Tight Reduction Techniques

Double the randomness.



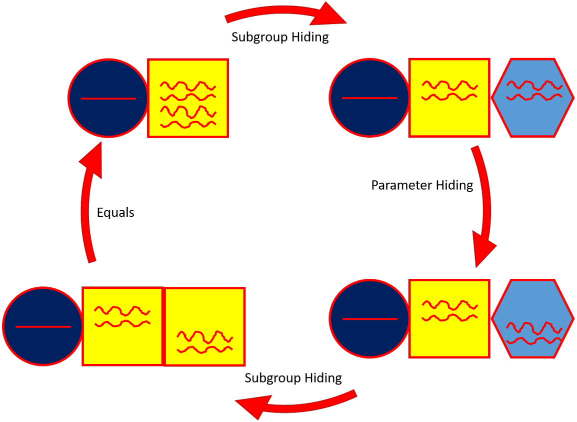
# Our Tight Reduction Techniques

Double the randomness.



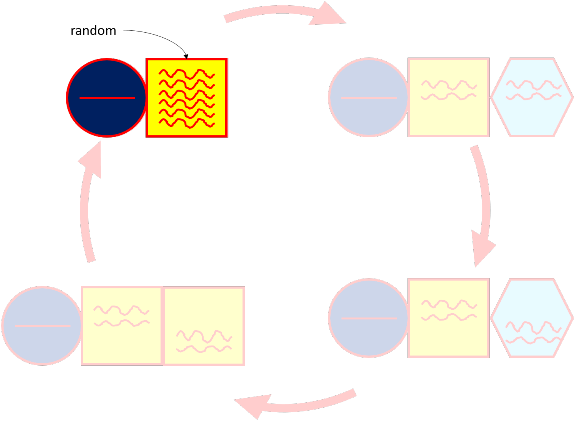
# Our Tight Reduction Techniques

Double the randomness.



# Our Tight Reduction Techniques

Double the randomness.



# Result

Given

$$g^{\rho_1(x)}, \ldots, g^{\rho_q(x)}, h^{\sigma_1(x)}, \ldots, h^{\sigma_q(x)}$$
$$\hat{h}$$

Then

$$\text{Adv}[\text{Deciding } e(g, \hat{h})^{f(x)} \text{ from random}] \leq (3 + \log(q+2)) \Pr[\text{Breaks Subgroup Hiding}]$$

# Result

Subgroup Hiding & Parameter Hiding $\Rightarrow$ Specific classes of $q$-type assumptions in asymmetric bilinear groups of order $N = p_1 p_2 p_3$.

$$\Pr[\text{break } q\text{-type assumption}] \leq \mathcal{O}(\log q) \Pr[\text{break subgroup hiding}]$$

# Outline of Presentation

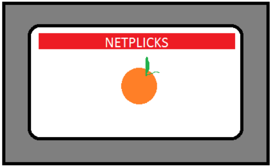
Bilinear Groups and Assumptions

Tight Reduction

Symmetric Schemes

Conclusion

# Example: Broadcast Encryption




Methods of delivering encrypted content over a broadcast channel where only qualified users can decrypt the content.

## Example

*Boneh Gentry and Waters′ broadcast encryption scheme [BGW-Crypto05].*

- *Pairing based solution*
- *Short ciphertexts and private keys*
- *Collusion resistant*

# Broadcast Encryption

The asymmetric $q$-BDHE assumption:

$$\text{given } \hat{h}, g^{\alpha}, h^{\alpha}, \ldots, g^{\alpha^q}, h^{\alpha^q}, g^{\alpha^{q+2}}, h^{\alpha^{q+2}}, \ldots, g^{\alpha^{2q}}, h^{\alpha^{2q}}$$
$$\text{it is hard to distinguish } e(g, \hat{h})^{q+1} \text{ from random}$$

is tightly implied by subgroup hiding and parameter hiding.

*The BGW broadcast encryption scheme is implied by the symmetric $q$-BDHE assumption.*

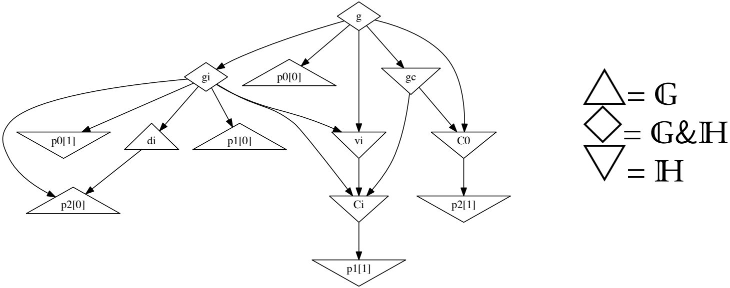
# Symmetric Reductions

- The previous asymmetric reduction fails in the symmetric case.
- Adversary given components that would allow it to trivially break subgroup hiding in the symmetric case ($e(\mathbb{G}_1, \mathbb{H}_2) = 1$).
- Show how to push through the same reduction in the symmetric case by adding randomness from a fourth subgroup.

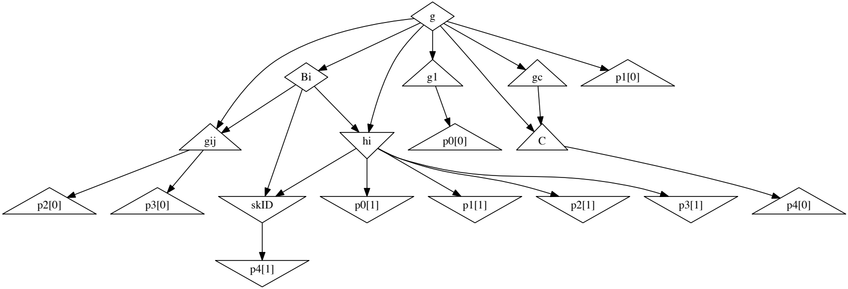
Symmetric schemes can also be translated into asymmetric groups.

# The Asymmetric BGW Variant

Techniques from [AGOT-Crypto14].

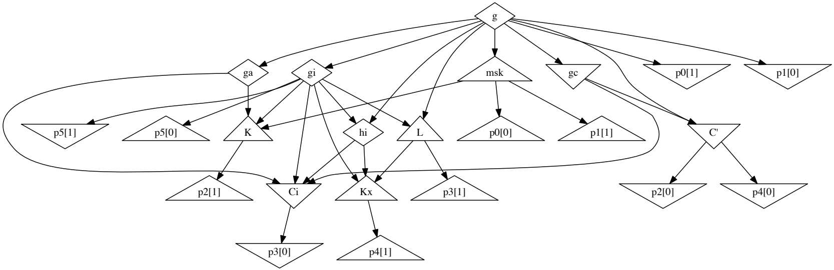


# Identity Based KEM [ACF-Eurocrypt09]

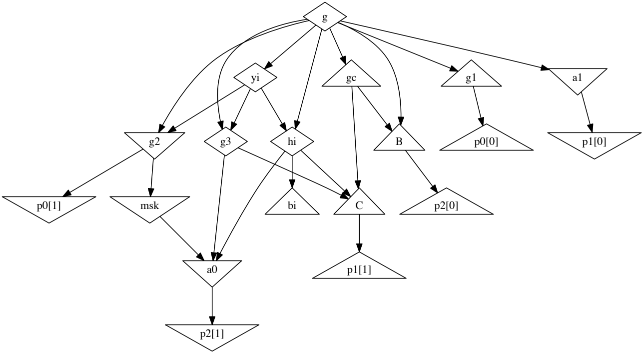


# ABE Scheme [Waters08]

The less efficient construction.



# HIBE Scheme [BBG-Eurocrypt05]



# Outline of Presentation

Bilinear Groups and Assumptions

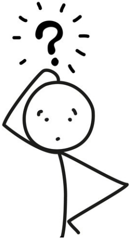
Tight Reduction

Symmetric Schemes

Conclusion

# Open Problems

- How secure are $q$-type assumptions in prime order groups?
- How secure are $q$-power knowledge of exponent assumptions (non-falsifiable assumptions)?
- How secure are $q$-type when the adversary has inputs from both source groups and the challenge component is also in the source group?



# Thank-you for Listening.