On the Statistical Leak of the GGH13 Multilinear Map and some Variants

Léo Ducas[1], **Alice Pellet-Mary**[2]

[1]Cryptology Group, CWI, Amsterdam

[2]LIP, ENS de Lyon

Asiacrypt 2018

What is this talk about?

Objective: Analyse the statistical leak of the GGH13 multilinear map

GGH13: Garg, Gentry and Halevi. Candidate multilinear maps from ideal lattices, Eurocrypt.

What is this talk about?

Objective: Analyse the statistical leak of the GGH13 multilinear map

- Description of a simple setting using the GGH13 map

GGH13: Garg, Gentry and Halevi. Candidate multilinear maps from ideal lattices, Eurocrypt.

What is this talk about?

Objective: Analyse the statistical leak of the GGH13 multilinear map

- Description of a simple setting using the GGH13 map
- Analyse of the statistical leak in this simple setting
  - For 4 different variants of the GGH13 map

GGH13: Garg, Gentry and Halevi. Candidate multilinear maps from ideal lattices, Eurocrypt.

What is this talk about?

Objective: Analyse the statistical leak of the GGH13 multilinear map

- Description of a simple setting using the GGH13 map
- Analyse of the statistical leak in this simple setting
  - For 4 different variants of the GGH13 map
- Proposition of a countermeasure

GGH13: Garg, Gentry and Halevi. Candidate multilinear maps from ideal lattices, Eurocrypt.

Cryptographic multilinear map

Definition: κ asymmetric multilinear map

Different levels of encodings, corresponding to subsets of $\{1, \dots, \kappa\}$.
Denote by $\mathsf{Enc}(a, S)$ a level-S encoding of the message a, for $S \subseteq \{1, \dots, \kappa\} =: [\kappa]$.

Cryptographic multilinear map

Definition: κ asymmetric multilinear map

Different levels of encodings, corresponding to subsets of $\{1, \ldots, \kappa\}$.
Denote by $\mathrm{Enc}(a, S)$ a level-S encoding of the message a, for $S \subseteq \{1, \ldots, \kappa\} =: [\kappa]$.

Functionality:

Addition: $\mathrm{Add}(\mathrm{Enc}(a_1, S), \mathrm{Enc}(a_2, S)) = \mathrm{Enc}(a_1 + a_2, S)$

Multiplication: $\mathrm{Mult}(\mathrm{Enc}(a_1, S_1), \mathrm{Enc}(a_2, S_2)) = \mathrm{Enc}(a_1 \cdot a_2, S_1 \cup S_2)$ if $S_1 \cap S_2 = \emptyset$

Zero-test: $\text{Zero-test}(\mathrm{Enc}(a, [\kappa])) = \text{True iff } a = 0$

Security: multiple security definitions

Mmap: applications and candidates

Applications:

- One-round key-exchange between $\kappa + 1$ users (generalization of pairings)
- Attribute based encryption, witness encryption, ...
- Indistinguishability obfuscation (iO)

Mmap: applications and candidates

Applications:

- One-round key-exchange between $\kappa + 1$ users (generalization of pairings)
- Attribute based encryption, witness encryption, ...
- Indistinguishability obfuscation (iO)

Three main candidates

GGH13, CLT13, GGH15

GGH13: Garg, Gentry and Halevi (Eurocrypt 2013)
CLT13: Coron, Lepoint, Tibouchi (Crypto 2013)
GGH15: Gentry, Gorbunov, Halevi (TCC 2015)

Previous attacks on GGH13 map

Zeroizing attacks

Theorem [Hu and Jia, Eurocrypt'16]

The GGH13 map is insecure if encodings of zero are provided.

Previous attacks on GGH13 map

Zeroizing attacks

Theorem [Hu and Jia, Eurocrypt'16]

The GGH13 map is insecure if encodings of zero are provided.

- GGH13 is insecure for almost all applications, **except** obfuscation.

Previous attacks on GGH13 map

Zeroizing attacks

Theorem [Hu and Jia, Eurocrypt'16]

The GGH13 map is insecure if encodings of zero are provided.

- GGH13 is insecure for almost all applications, **except** obfuscation.
- Zeroizing attack on some candidate obfuscators:
  - Miles, Sahai, Zhandry, Crypto'16
  - Chen, Gentry, Halevi, EC'17

Previous attacks on GGH13 map

Zeroizing attacks

Theorem [Hu and Jia, Eurocrypt'16]

The GGH13 map is insecure if encodings of zero are provided.

- GGH13 is insecure for almost all applications, **except** obfuscation.
- Zeroizing attack on some candidate obfuscators:
  - Miles, Sahai, Zhandry, Crypto'16
  - Chen, Gentry, Halevi, EC'17

Statistical attacks

Previous attacks on GGH13 map

Zeroizing attacks

Theorem [Hu and Jia, Eurocrypt'16]
The GGH13 map is insecure if encodings of zero are provided.

- GGH13 is insecure for almost all applications, **except** obfuscation.
- Zeroizing attack on some candidate obfuscators:
  - Miles, Sahai, Zhandry, Crypto'16
  - Chen, Gentry, Halevi, EC'17

Statistical attacks

- mentioned in [GGH13]
  - 2 sampling methods proposed

What is a statistical attack?

In the GGH13 map:

- Encodings are randomized **but** modulo q
  - analogous to NTRU
  - expectation and variance reveal nothing

What is a statistical attack?

In the GGH13 map:

- Encodings are randomized **but** modulo q
  - analogous to NTRU
  - expectation and variance reveal nothing
- After zero-test: obtain an element in $\mathbb{Z}$ (no reduction $\bmod q$)
  - function of the encodings

What is a statistical attack?

In the GGH13 map:

- Encodings are randomized **but** modulo q
  - analogous to NTRU
  - expectation and variance reveal nothing
- After zero-test: obtain an element in $\mathbb{Z}$ (no reduction $\bmod q$)
  - function of the encodings
  - hence randomized
  - its variance might reveal secret information

What is a statistical attack?

In the GGH13 map:

- Encodings are randomized **but** modulo q
  - analogous to NTRU
  - expectation and variance reveal nothing
- After zero-test: obtain an element in $\mathbb{Z}$ (no reduction $\bmod q$)
  - function of the encodings
  - hence randomized
  - its variance might reveal secret information

In this talk

The leak we analyse is the variance of the post-zero-tested elements

Contribution (1)

What setting of the GGH13 map should we consider?

Contribution (1)

What setting of the GGH13 map should we consider?

We define our own setting

Contribution (1)

What setting of the GGH13 map should we consider?

We define our own setting

- inspired by iO

Contribution (1)

What setting of the GGH13 map should we consider?

We define our own setting

- inspired by iO
- but simpler

Contribution (1)

What setting of the GGH13 map should we consider?

We define our own setting

- inspired by iO
- but simpler
- secure in the weak multilinear map model
  - no "simple" zeroizing attacks

Contribution (2)

- We consider 4 different sampling procedures for the encodings:
  - 2 from [GGH13]
  - 2 from [DGG+18]

[DGG+18] Döttling, Garg, Gupta, Miao, and Mukherjee. Obfuscation from Low Noise Multilinear Maps, Indocrypt.

Contribution (2)

- We consider 4 different sampling procedures for the encodings:
  - 2 from [GGH13]
  - 2 from [DGG+18]

Sampling method	leakage related to secret elements	full attack?
Simplistic [GGH13]	yes	yes for some params
Exponential [GGH13]	yes	no
Conservative [DGG+18]	yes	no
Aggressive [DGG+18]	yes	no

[DGG+18] Döttling, Garg, Gupta, Miao, and Mukherjee. Obfuscation from Low Noise Multilinear Maps, Indocrypt.

Contribution (2)

- We consider 4 different sampling procedures for the encodings:
  - 2 from [GGH13]
  - 2 from [DGG+18]

Sampling method	leakage related to secret elements	full attack?
Simplistic [GGH13]	yes	yes for some params
Exponential [GGH13]	yes	no
Conservative [DGG+18]	yes	no
Aggressive [DGG+18]	yes	no
Compensation (this work)	no	no

- We propose a countermeasure ⇒ Compensation method
  - In **this** simple setting
  - Almost as efficient as the simplistic method

[DGG+18] Döttling, Garg, Gupta, Miao, and Mukherjee. Obfuscation from Low Noise Multilinear Maps, Indocrypt.

Outline of the talk

The GGH13 multilinear map

- Define $R = \mathbb{Z}[X]/(X^n + 1)$ with $n = 2^k$

The GGH13 multilinear map

- Define $R = \mathbb{Z}[X]/(X^n + 1)$ with $n = 2^k$
- Sample g a “small” element in R
  $\Rightarrow$ the plaintext space is $\mathcal{P} = R/\langle g \rangle$

The GGH13 multilinear map

- Define $R = \mathbb{Z}[X]/(X^n + 1)$ with $n = 2^k$
- Sample g a "small" element in R
  $\Rightarrow$ the plaintext space is $\mathcal{P} = R/\langle g \rangle$
- Sample q a "large" integer
  $\Rightarrow$ the encoding space is $R_q = R/(qR) = \mathbb{Z}_q[X]/(X^n + 1)$

Notation

We write $[r]_q$ for the elements in R_q

The GGH13 multilinear map: encodings

- Sample $z_1, \dots, z_\kappa$ uniformly in R_q
- **Encoding:** An encoding of a at level $S \subseteq \{1, \dots, \kappa\}$ is

$$u = \left[\frac{\widetilde{a}}{\prod_{i \in S} z_i} \right]_q$$

where $\widetilde{a} = a \bmod g$

The GGH13 multilinear map: encodings

- Sample $z_1, \ldots, z_\kappa$ uniformly in R_q
- **Encoding:** An encoding of a at level $S \subseteq \{1, \ldots, \kappa\}$ is

$$u = \left[\frac{\widetilde{a}}{\prod_{i \in S} z_i} \right]_q$$

where $\widetilde{a} = a \bmod g$

Addition and multiplication

Addition:

$$\left[\frac{a_1 + r_1 g}{\prod_{i \in S} z_i} \right]_q + \left[\frac{a_2 + r_2 g}{\prod_{i \in S} z_i} \right]_q = \left[\frac{a_1 + a_2 + r' g}{\prod_{i \in S} z_i} \right]_q$$

Multiplication:

$$\left[\frac{a_1 + r_1 g}{\prod_{i \in S_1} z_i} \right]_q \cdot \left[\frac{a_2 + r_2 g}{\prod_{i \in S_2} z_i} \right]_q = \left[\frac{a_1 \cdot a_2 + r' g}{\prod_{i \in S_1 \cup S_2} z_i} \right]_q \quad (\text{if } S_1 \cap S_2 = \emptyset)$$

The GGH13 multilinear map: zero-test

- Sample h in R of the order of $q^{1/2}$
- Let $z^* = \prod_{i=1}^{\kappa} z_i$
- Define

$$p_{zt} = [z^* h g^{-1}]_q$$

The GGH13 multilinear map: zero-test

- Sample h in R of the order of $q^{1/2}$
- Let $z^* = \prod_{i=1}^{\kappa} z_i$
- Define

$$p_{zt} = [z^* h g^{-1}]_q$$

Zero-test

To test if $u = [c/z^*]_q$ is an encoding of zero (i.e. $c = 0 \mod g$), compute

$$[u \cdot p_{zt}]_q = [chg^{-1}]_q$$

This is small iff c is a small multiple of g.

Remark: If $c = 0 \mod g$, then $\boxed{[u \cdot p_{zt}]_q = ch/g \text{ over } R}$

Outline of the talk

1 The GGH13 Map

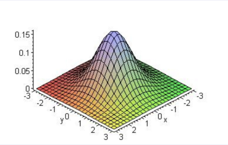
2 Statistical Leak

Statistical background (1)

Definitions

A distribution is said **centered** if its mean is zero.
A distribution is said **isotropic** if no direction is privileged.

Example



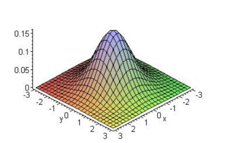
Notation: We write in red the centered isotropic variables

Statistical background (1)

Definitions

A distribution is said **centered** if its mean is zero.
A distribution is said **isotropic** if no direction is privileged.

Example



Notation: We write in red the centered isotropic variables

Gaussian distribution

We write $D_{L,\sigma}$ the discrete Gaussian distribution centered in 0 and of variance parameter σ^2 over the lattice L

$D_{L,\sigma}$ is a centered isotropic distribution

Statistical background (2)

Definitions / Notation

- For $r \in R$, we denote $A(r) = r\bar{r}$ the **auto-correlation** of r, where $\bar{r}$ is the complex conjugate of r when seen in $\mathbb{C}$
- The **variance** of a centered variable r is $\text{Var}(r) := \mathbb{E}(r\bar{r})$

Statistical background (2)

Definitions / Notation

- For $r \in R$, we denote $A(r) = r\bar{r}$ the **auto-correlation** of r, where $\bar{r}$ is the complex conjugate of r when seen in $\mathbb{C}$
- The **variance** of a centered variable r is $\mathrm{Var}(r) := \mathbb{E}(r\bar{r})$

Proposition: If r is centered and isotropic then

$$\mathbb{E}(r) = 0$$
$$\mathrm{Var}(r) = \mu \in \mathbb{R}$$

Statistical background (2)

Definitions / Notation

- For $r \in R$, we denote $A(r) = r\bar{r}$ the **auto-correlation** of r, where $\bar{r}$ is the complex conjugate of r when seen in $\mathbb{C}$
- The **variance** of a centered variable r is $\mathrm{Var}(r) := \mathbb{E}(r\bar{r})$

Proposition: If r is centered and isotropic then

$$\mathbb{E}(r) = 0$$

$$\sout{\mathrm{Var}(r) = \mu \in \mathbb{R}}$$

In this talk, assume $\mathrm{Var}(r) = 1$

Statistical leak

Recall

If $u = [c/z^*]_q$ with $c = 0 \bmod g$, then

$$[u \cdot p_{zt}]_q = c \cdot h/g \in R$$

Statistical leak

Recall

If $u = [c/z^*]_q$ with $c = 0 \bmod g$, then

$$[u \cdot p_{zt}]_q = c \cdot h/g \in R$$

Idea: h/g is fixed but c is a random variable

$$\boxed{\mathrm{Var}(c \cdot h/g) = \mathrm{Var}(c) \cdot A(h/g)}$$

We can approximate it with many samples

Simple setting (simplified)

- For all $1 \leq i \leq \kappa$, we get
  - $[\frac{\widetilde{a_i}}{z_i}]_q$ with $\widetilde{a_i} = a_i \bmod g$
  - $[\frac{\widetilde{b_i}}{\prod_{j \neq i} z_j}]_q$ with $\widetilde{b_i} = b_i \bmod g$
- such that $a_i b_i = 0$

1	2	3	$\cdots$	i	$\cdots$	κ

a_i

b_i

$a_i b_i = 0$

Leak in the simple setting

We get encodings of zero:

$$u_i = \left[\frac{\widetilde{a}_i}{z_i}\right]_q \cdot \left[\frac{\widetilde{b}_i}{\prod_{j \neq i} z_j}\right]_q = \left[\frac{\widetilde{a}_i \widetilde{b}_i}{z^*}\right]_q$$

Leak in the simple setting

We get encodings of zero:

$$u_i = \left[\frac{\widetilde{a_i}}{z_i}\right]_q \cdot \left[\frac{\widetilde{b_i}}{\prod_{j \neq i} z_j}\right]_q = \left[\frac{\widetilde{a_i}\widetilde{b_i}}{z^*}\right]_q$$

After zero-test:

$$(\widetilde{a_i} \cdot \widetilde{b_i}) \cdot h/g \in R$$

Leak in the simple setting

We get encodings of zero:

$$u_i = \left[\frac{\widetilde{a}_i}{z_i}\right]_q \cdot \left[\frac{\widetilde{b}_i}{\prod_{j \neq i} z_j}\right]_q = \left[\frac{\widetilde{a}_i \widetilde{b}_i}{z^*}\right]_q$$

After zero-test:

$$(\widetilde{a}_i \cdot \widetilde{b}_i) \cdot h/g \in R$$

Variance:

$$\mathrm{Var}(\widetilde{a}_i \cdot \widetilde{b}_i) \cdot A(h/g) = \mathrm{Var}(\widetilde{a}_i) \cdot \mathrm{Var}(\widetilde{b}_i) \cdot A(h/g)$$

Leakage for the two methods of [GGH13]

Recall

The leakage is

$$\mathrm{Var}(\widetilde{a_i}) \cdot \mathrm{Var}(\widetilde{b_i}) \cdot A(h/g)$$

Leakage for the two methods of [GGH13]

Recall

The leakage is

$$\mathrm{Var}(\widetilde{a_i}) \cdot \mathrm{Var}(\widetilde{b_i}) \cdot A(h/g)$$

The simplistic method:

$\widetilde{a_i} \leftarrow D_{a_i+gR,\sigma}$

$\widetilde{b_i} \leftarrow D_{b_i+gR,\sigma}$

Leakage for the two methods of [GGH13]

Recall

The leakage is

$$\mathrm{Var}(\widetilde{a_i}) \cdot \mathrm{Var}(\widetilde{b_i}) \cdot A(h/g)$$

The simplistic method:

$\widetilde{a_i} \leftarrow D_{a_i+gR,\sigma}$

$\widetilde{b_i} \leftarrow D_{b_i+gR,\sigma}$

Leakage: $A(h/g)$

Leakage for the two methods of [GGH13]

Recall

The leakage is

$$\mathrm{Var}(\widetilde{a_i}) \cdot \mathrm{Var}(\widetilde{b_i}) \cdot A(h/g)$$

The simplistic method:

$$\widetilde{a_i} \leftarrow D_{a_i+gR,\sigma}$$
$$\widetilde{b_i} \leftarrow D_{b_i+gR,\sigma}$$

Leakage: $A(h/g)$

The exponential method:

$$\widetilde{a_i} = \widehat{a_i} \cdot z_i$$
$$\widetilde{b_i} = \widehat{b_i} \cdot \prod_{j \neq i} z_j$$
$$\text{for } \widehat{a_i} \leftarrow D_{(a_i+gR)/z_i,\ \sigma}$$
$$\widehat{b_i} \leftarrow D_{(b_i+gR)/(\prod_{j\neq i} z_j),\ \sigma}$$

Leakage for the two methods of [GGH13]

Recall

The leakage is
$$\mathrm{Var}(\widetilde{a_i}) \cdot \mathrm{Var}(\widetilde{b_i}) \cdot A(h/g)$$

The simplistic method:

$$\widetilde{a_i} \leftarrow D_{a_i+gR,\sigma}$$
$$\widetilde{b_i} \leftarrow D_{b_i+gR,\sigma}$$

Leakage: $A(h/g)$

The exponential method:

$$\widetilde{a_i} = \widehat{a_i} \cdot z_i$$
$$\widetilde{b_i} = \widehat{b_i} \cdot \prod_{j \neq i} z_j$$
$$\text{for } \widehat{a_i} \leftarrow D_{(a_i+gR)/z_i,\ \sigma}$$
$$\widehat{b_i} \leftarrow D_{(b_i+gR)/(\prod_{j\neq i} z_j),\ \sigma}$$

Leakage:

$$A(z_i) \cdot A(\prod_{j \neq i} z_j) \cdot A(h/g)$$
$$= A(z^* h/g)$$

Countermeasure

Recall

The leakage is

$$\mathrm{Var}(\widetilde{a_i}) \cdot \mathrm{Var}(\widetilde{b_i}) \cdot A(h/g)$$

Wanted: $\mathrm{Var}(\widetilde{a_i}) \cdot \mathrm{Var}(\widetilde{b_i}) \cdot A(h/g) = 1$

Countermeasure

Recall

The leakage is
$$\mathrm{Var}(\widetilde{a_i}) \cdot \mathrm{Var}(\widetilde{b_i}) \cdot A(h/g)$$

Wanted: $\mathrm{Var}(\widetilde{a_i}) \cdot \mathrm{Var}(\widetilde{b_i}) \cdot A(h/g) = 1$

The compensation method:

$$\widetilde{a_i} = \widehat{a_i} \cdot \sqrt{g/h}$$
$$\widetilde{b_i} = \widehat{b_i} \cdot \sqrt{g/h}$$
$$\text{for } \widehat{a_i} \leftarrow D_{(a_i+gR)/\sqrt{g/h},\ \sigma}$$
$$\widehat{b_i} \leftarrow D_{(b_i+gR)/\sqrt{g/h},\ \sigma}$$

Countermeasure

Recall

The leakage is
$$\mathrm{Var}(\widetilde{a_i}) \cdot \mathrm{Var}(\widetilde{b_i}) \cdot A(h/g)$$

Wanted: $\mathrm{Var}(\widetilde{a_i}) \cdot \mathrm{Var}(\widetilde{b_i}) \cdot A(h/g) = 1$

The compensation method:

$$\widetilde{a_i} = \widehat{a_i} \cdot \sqrt{g/h}$$
$$\widetilde{b_i} = \widehat{b_i} \cdot \sqrt{g/h}$$
$$\text{for } \widehat{a_i} \leftarrow D_{(a_i+gR)/\sqrt{g/h},\ \sigma}$$
$$\widehat{b_i} \leftarrow D_{(b_i+gR)/\sqrt{g/h},\ \sigma}$$

Leakage:

$$A(\sqrt{g/h}) \cdot A(\sqrt{g/h}) \cdot A(h/g)$$
$$= 1$$

Remark: more efficient than other methods (except simplistic)

What to do with the leakage

	Simplistic method	Exponential method
Leakage	$\approx A(h/g)$	$\approx A(z^* h/g)$

Problem: The leaked values are fractions

What to do with the leakage

	Simplistic method	Exponential method
Leakage	$\approx A(h/g)$	$\approx A(z^* h/g)$

Problem: The leaked values are fractions

Solution: for the simplistic method

- Zero-test $\Rightarrow$ recover multiple of h: $r \cdot h$

What to do with the leakage

	Simplistic method	Exponential method
Leakage	$\approx A(h/g)$	$\approx A(z^* h/g)$

Problem: The leaked values are fractions

Solution: for the simplistic method

- Zero-test $\Rightarrow$ recover multiple of h: $r \cdot h$
- Combine it with the leakage to get: $\approx A(rg)$
  - Integer coefficients

What to do with the leakage

	Simplistic method	Exponential method
Leakage	$\approx A(h/g)$	$\approx A(z^* h/g)$

Problem: The leaked values are fractions

Solution: for the simplistic method

- Zero-test $\Rightarrow$ recover multiple of h: $r \cdot h$
- Combine it with the leakage to get: $\approx A(rg)$
  - Integer coefficients
- If q is poly(n)
  - $A(rg)$ is poly(n)
  - it can be recovered exactly with polynomially many samples
  - obtain a multiple of g

What to do with the leakage

	Simplistic method	Exponential method
Leakage	$\approx A(h/g)$	$\approx A(z^* h/g)$

Problem: The leaked values are fractions

Solution: for the simplistic method

- Zero-test $\Rightarrow$ recover multiple of h: $r \cdot h$
- Combine it with the leakage to get: $\approx A(rg)$
  - Integer coefficients
- If q is poly(n)
  - $A(rg)$ is poly(n)
  - it can be recovered exactly with polynomially many samples
  - obtain a multiple of g

Remark: does not work for $A(z^* h/g)$

Conclusion

Sampling method	leakage	full attack?
Simplistic [GGH13]	$A(h/g)$	yes if q is poly
Exponential [GGH13]	$A(z^* h/g)$	no
Conservative [DGG+18]	$A(h/g)$	no
Aggressive [DGG+18]	$A(z^* h/g)$	no
Compensation (this work)	1	no

Conclusion

Sampling method	leakage	full attack?
Simplistic [GGH13]	$A(h/g)$	yes if q is poly
Exponential [GGH13]	$A(z^* h/g)$	no
Conservative [DGG+18]	$A(h/g)$	no
Aggressive [DGG+18]	$A(z^* h/g)$	no
Compensation (this work)	1	no

Open problems:

- Make the full attack work for the conservative method?

Conclusion

Sampling method	leakage	full attack?
Simplistic [GGH13]	$A(h/g)$	yes if q is poly
Exponential [GGH13]	$A(z^* h/g)$	no
Conservative [DGG+18]	$A(h/g)$	no
Aggressive [DGG+18]	$A(z^* h/g)$	no
Compensation (this work)	1	no

Open problems:

- Make the full attack work for the conservative method?
- Is the leak $A(z^* h/g)$ critical?

Conclusion

Sampling method	leakage	full attack?
Simplistic [GGH13]	$A(h/g)$	yes if q is poly
Exponential [GGH13]	$A(z^* h/g)$	no
Conservative [DGG$^+$18]	$A(h/g)$	no
Aggressive [DGG$^+$18]	$A(z^* h/g)$	no
Compensation (this work)	1	no

Open problems:

- Make the full attack work for the conservative method?
- Is the leak $A(z^* h/g)$ critical?
- Extend the simple setting
  - Is the compensation method still safe in other settings?

Conclusion

Sampling method	leakage	full attack?
Simplistic [GGH13]	$A(h/g)$	yes if q is poly
Exponential [GGH13]	$A(z^* h/g)$	no
Conservative [DGG+18]	$A(h/g)$	no
Aggressive [DGG+18]	$A(z^* h/g)$	no
Compensation (this work)	1	no

Open problems:

- Make the full attack work for the conservative method?
- Is the leak $A(z^* h/g)$ critical?
- Extend the simple setting
  - Is the compensation method still safe in other settings?

Questions?