A Simple Framework for Noise-Free Construction of Fully Homomorphic Encryption from a Special Class of Non-Commutative Groups

Koji Nuida

National Institute of Advanced Industrial Science and Technology (AIST), Japan
(Japan Science and Technology Agency (JST) PRESTO Researcher)

Mathematics of Cryptography @ UCI September 1, 2015

Summary of Talk

- Proposal of FHE without bootstrapping, based on non-commutative groups (ePrint 2014/097)
  - Homomorphic operators from commutator with rerandomized inputs
  - Constructing underlying groups by group presentations (generators and their relations)
  - "Obfuscating" group structure by random transformations of group presentation
- Candidate choice of groups
  - Attacks for inappropriate groups

Contents

Contents

Fully Homomorphic Encryption (FHE)

- PKE + "any computation on encrypted data"
  - "Homomorphic operation" on ciphertexts
- In this talk: Plaintext $m \in \{0, 1\}$, and

$$\begin{aligned}
\mathrm{Dec}(\mathrm{Enc}(m)) &= m \\
\mathrm{Dec}(\mathrm{NOT}(c)) &= \neg\mathrm{Dec}(c) \\
\mathrm{Dec}(\mathrm{AND}(c_1, c_2)) &= \mathrm{Dec}(c_1) \wedge \mathrm{Dec}(c_2)
\end{aligned}$$

except negligible error prob.

Example: [van Dijk et al. EC'10]

- Ciphertext for $m \in \{0, 1\}$: $c = pq + 2r + m$
  - $\mathrm{Dec}(c) = (c \bmod p) \bmod 2$
- Homomorphic $+$ and $\times$ preserve shapes of ciphertexts, **but "noise" r amplified**

Example: [van Dijk et al. EC'10]

- Ciphertext for $m \in \{0, 1\}$: $c = pq + 2r + m$
  - $\mathrm{Dec}(c) = (c \bmod p) \bmod 2$
- Homomorphic $+$ and $\times$ preserve shapes of ciphertexts, **but "noise" r amplified**
- Finally yielding dec. failure! (Somewhat HE)
  - Noise reduction required: "**Bootstrapping**" ([Gentry STOC'09])

Bootstrapping

- Opened the heavy door to FHE, but:
  - Computationally inefficient (despite e.g., [Ducas–Micciancio EC'15])
  - Syntax less analogical to classical HE
  - Problem of circular security

Bootstrapping

- Opened the heavy door to FHE, but:
  - Computationally inefficient (despite e.g., [Ducas–Micciancio EC'15])
  - Syntax less analogical to classical HE
  - Problem of circular security
- **Goal: FHE without bootstrapping**
  - No (acknowledged) solutions so far

Non-Commutative Groups and Commutator

- We use finite **non-commutative** groups G
  - Multiplicative, with identity element $1 = 1_G$
- **Commutator** defined on G:

$$[g, h] = g \cdot h \cdot g^{-1} \cdot h^{-1}$$

  - $[g, h] = 1$ if $gh = hg$
  - Always $[g, h] = 1$ if G is commutative

Strategy Outline

1. Realize homomorphic operators in group $\overline{G}$
   - By composing group operators in $\overline{G}$
2. "Lift" the structure to large group G
   - With "trapdoor" homomorphism $\varphi \colon G \twoheadrightarrow \overline{G}$
   - Homomorphic operators are "compatible" with φ, hence lifted to G
3. "Obfuscate" group structure of G

Contents

Commutator and AND Operator

- $[g, h] = g \cdot h \cdot g^{-1} \cdot h^{-1}$
- $(g = 1$ or $h = 1)$ implies $[g, h] = 1$

Commutator and AND Operator

- $[g, h] = g \cdot h \cdot g^{-1} \cdot h^{-1}$
- $(g = 1$ or $h = 1)$ implies $[g, h] = 1$
- Similar to: $(b = 0$ or $b' = 0)$ implies $b \wedge b' = 0$
  - Starting point of this work

Homomorphic NOT Operator

- $\overline{c} = (\overline{c_1}, \overline{c_2}) \in \overline{G} \times \overline{G}$ associated to $m \in \{0, 1\}$:
  - "Class-0" if $\overline{c_2} = 1$, "Class-1" if $\overline{c_2} = \overline{c_1}$
  - And $\overline{c_1} \neq 1$, to distinguish two classes
- Our NOT operator:

$$\overline{c} \mapsto (\overline{c_1}, \overline{c_1} \cdot (\overline{c_2})^{-1})$$

  - Switching class-0 and class-1

Homomorphic AND Operator?

- Given: Class-m $\overline{c}$ and class-m' $\overline{d}$
- Our homomorphic AND operator?

$$?? \quad (\overline{c}, \overline{d}) \mapsto \overline{e}\,,\ \overline{e_i} = [\overline{c_i}, \overline{d_i}]\ (i = 1, 2) \quad ??$$

- Given: Class-m $\overline{c}$ and class-m' $\overline{d}$
- Our homomorphic AND operator?

$$?? \quad (\overline{c}, \overline{d}) \mapsto \overline{e} \,,\; \overline{e_i} = [\overline{c_i}, \overline{d_i}] \; (i = 1, 2) \quad ??$$

- $\overline{e}$ is **almost** class-$(m \wedge m')$:
  - $m = 0$ implies $\overline{c_2} = 1$, $\overline{e_2} = 1$ $(0 \wedge m' = 0)$
  - $m' = 0$ implies $\overline{d_2} = 1$, $\overline{e_2} = 1$ $(m \wedge 0 = 0)$
  - $m = m' = 1$ implies $\overline{c_2} = \overline{c_1}$ and $\overline{d_2} = \overline{d_1}$, so $\overline{e_2} = \overline{e_1}$ $(1 \wedge 1 = 1)$

Homomorphic AND Operator?

- Given: Class-m $\overline{c}$ and class-m' $\overline{d}$
- Our homomorphic AND operator?

$$?? \quad (\overline{c}, \overline{d}) \mapsto \overline{e}\,,\ \overline{e_i} = [\overline{c_i}, \overline{d_i}]\ (i = 1, 2) \quad ??$$

- $\overline{e}$ is **almost** class-$(m \wedge m')$:
  - $m = 0$ implies $\overline{c_2} = 1$, $\overline{e_2} = 1$ $(0 \wedge m' = 0)$
  - $m' = 0$ implies $\overline{d_2} = 1$, $\overline{e_2} = 1$ $(m \wedge 0 = 0)$
  - $m = m' = 1$ implies $\overline{c_2} = \overline{c_1}$ and $\overline{d_2} = \overline{d_1}$, so $\overline{e_2} = \overline{e_1}$ $(1 \wedge 1 = 1)$
- But $\overline{e_1} \neq 1$ **not guaranteed** (e.g., $\overline{c_1} = \overline{d_1}$)

Homomorphic AND Operator

- ToDo: Avoid commuting $\overline{c_1}, \overline{d_1}$ in inputs

Homomorphic AND Operator

- ToDo: Avoid commuting $\overline{c_1}, \overline{d_1}$ in inputs
- Solution: "Rerandomize" the inputs as

$$\overline{e_1} = [\overline{g} \cdot \overline{c_1} \cdot (\overline{g})^{-1}, \overline{d_1}]$$
$$\overline{e_2} = [\overline{g} \cdot \overline{c_2} \cdot (\overline{g})^{-1}, \overline{d_2}]$$

($\overline{g} \in \overline{G}$ common and uniformly random)

- $\overline{e_2}$ still OK; $\overline{g} \cdot 1 \cdot (\overline{g})^{-1} = 1$, common $\overline{g}$ used

Homomorphic AND Operator

- ToDo: Avoid commuting $\overline{c_1}, \overline{d_1}$ in inputs
- Solution: "Rerandomize" the inputs as

$$\overline{e_1} = [\overline{g} \cdot \overline{c_1} \cdot (\overline{g})^{-1}, \overline{d_1}]$$
$$\overline{e_2} = [\overline{g} \cdot \overline{c_2} \cdot (\overline{g})^{-1}, \overline{d_2}]$$

  ($\overline{g} \in \overline{G}$ common and uniformly random)
- $\overline{e_2}$ still OK; $\overline{g} \cdot 1 \cdot (\overline{g})^{-1} = 1$, common $\overline{g}$ used
- $\overline{e_1}$ will be OK **if $\overline{G}$ is appropriate**

- **Definition** $\overline{G}$ is commutator-separable, if there is an exceptional subset $1 \in X \subset \overline{G}$ with:

- **Definition** $\overline{G}$ is commutator-separable, if there is an exceptional subset $1 \in X \subset \overline{G}$ with:
  - $|X|/|\overline{G}|$ negligible (so is $1/|\overline{G}|$)
    - Correctness of Enc

- **Definition** $\overline{G}$ is commutator-separable, if there is an exceptional subset $1 \in X \subset \overline{G}$ with:
  - $|X|/|\overline{G}|$ negligible (so is $1/|\overline{G}|$)
    - Correctness of Enc
  - For any $x, y \in \overline{G} \setminus X$,

$$\Pr[\ [gxg^{-1}, y] \in X\ ] \leq \mathrm{neg.}$$

  where $g \in \overline{G}$ is uniformly random
    - AND keeps $\overline{c_1} \notin X$ (hence $\overline{c_1} \neq 1$)

- **Definition** $\overline{G}$ is commutator-separable, if there is an exceptional subset $1 \in X \subset \overline{G}$ with:
  - $|X|/|\overline{G}|$ negligible (so is $1/|\overline{G}|$)
    - Correctness of Enc
  - For any $x, y \in \overline{G} \setminus X$,

$$\Pr[\ [gxg^{-1}, y] \in X\ ] \leq \mathrm{neg}.$$

    where $g \in \overline{G}$ is uniformly random
    - AND keeps $\overline{c_1} \notin X$ (hence $\overline{c_1} \neq 1$)
- Examples: $\mathrm{SL}_2(\mathbb{F}_q)$, $\mathrm{PSL}_2(\mathbb{F}_q)$, $1/q$ neg.

- $\Pr[\ [gxg^{-1}, y] \in X\ ] \leq \dfrac{|X| \cdot |Z_{\overline{G}}(x)| \cdot |Z_{\overline{G}}(y)|}{|\overline{G}|}$,
  where $Z_{\overline{G}}(x) = \{z \in \overline{G} \mid xz = zx\}$

Examples of $\overline{G}$

- $\Pr[\ [gxg^{-1}, y] \in X\ ] \leq \dfrac{|X| \cdot |Z_{\overline{G}}(x)| \cdot |Z_{\overline{G}}(y)|}{|\overline{G}|}$, where $Z_{\overline{G}}(x) = \{z \in \overline{G} \mid xz = zx\}$
- $|\mathrm{SL}_2(\mathbb{F}_q)| = q(q^2 - 1)$
- For $\overline{G} = \mathrm{SL}_2(\mathbb{F}_q)$, $|Z_{\overline{G}}(x)| \leq 2q$ for $x \neq \pm I$

Examples of $\overline{G}$

- $\Pr[\ [gxg^{-1}, y] \in X\ ] \le \dfrac{|X| \cdot |Z_{\overline{G}}(x)| \cdot |Z_{\overline{G}}(y)|}{|\overline{G}|}$,
  where $Z_{\overline{G}}(x) = \{z \in \overline{G} \mid xz = zx\}$
- $|\mathrm{SL}_2(\mathbb{F}_q)| = q(q^2 - 1)$
- For $\overline{G} = \mathrm{SL}_2(\mathbb{F}_q)$, $|Z_{\overline{G}}(x)| \le 2q$ for $x \ne \pm I$
- Hence commutator-separable, with $X = \{\pm I\}$
  - So is $\mathrm{PSL}_2(\mathbb{F}_q) = \mathrm{SL}_2(\mathbb{F}_q)/\{\pm I\}$, $X = 1$

The Scheme

- Given: $\varphi\colon G \to \overline{G}$ ($\overline{G}$ commutator-separable), uniformly random sampling algorithms Sample_G for G and Sample_N for $N = \ker\varphi$
- $\mathsf{pk} = (G, \mathsf{Sample}_G, \mathsf{Sample}_H)$, $\mathsf{sk} = \varphi$
- $\mathsf{Enc}(m) = (c_1, {c_1}^m \cdot h)$, $c_1 \leftarrow G$, $h \leftarrow N$
- $\mathsf{Dec}(c = (c_1, c_2)) = \begin{cases} 0 & \text{if } \varphi(c_2) = \overline{c_2} = 1_{\overline{G}} \\ 1 & \text{otherwise} \end{cases}$
- $\mathsf{NOT}(c) = (c_1, c_1 \cdot {c_2}^{-1})$
- $\mathsf{AND}(c, d) = ([gc_1g^{-1}, d_1], [gc_2g^{-1}, d_2])$, $g \leftarrow G$

Generalization

- Motivation: Can we use S_n or A_n as $\overline{G}$?

- Motivation: Can we use S_n or A_n as $\overline{G}$?
- Let $\overline{G}$ be finite, non-commutative and simple
- **Fact** [Guralnick–Robinson '06]
  $\Pr[\ [x,y] = 1\ ] \leq |\overline{G}|^{-1/2}$ for $x, y \leftarrow \overline{G}$

Generalization

- Motivation: Can we use S_n or A_n as $\overline{G}$?
- Let $\overline{G}$ be finite, non-commutative and simple
- **Fact** [Guralnick–Robinson '06]
  $\Pr[\ [x,y] = 1\ ] \leq |\overline{G}|^{-1/2}$ for $x, y \leftarrow \overline{G}$
- **Assumption** For $1 \neq x \in \overline{G}$, distribution of
  $F(x) = (g_1 x {g_1}^{-1})^{\varepsilon_1} \cdots (g_\ell x {g_\ell}^{-1})^{\varepsilon_\ell}$ for random
  $g_i \in \overline{G}$, $\varepsilon_i \in \mathbb{Z}$ is statistically close to uniform
  - $\overline{G}$ is generated by such $g_i x {g_i}^{-1}$

Generalization

- Motivation: Can we use S_n or A_n as $\overline{G}$?
- Let $\overline{G}$ be finite, non-commutative and simple
- **Fact** [Guralnick–Robinson '06]
  $\Pr[\ [x,y] = 1\ ] \leq |\overline{G}|^{-1/2}$ for $x, y \leftarrow \overline{G}$
- **Assumption** For $1 \neq x \in \overline{G}$, distribution of $F(x) = ({g_1 x g_1}^{-1})^{\varepsilon_1} \cdots ({g_\ell x g_\ell}^{-1})^{\varepsilon_\ell}$ for random $g_i \in \overline{G}$, $\varepsilon_i \in \mathbb{Z}$ is statistically close to uniform
  - $\overline{G}$ is generated by such ${g_i x g_i}^{-1}$
- Then $\mathrm{AND}(\overline{c}, \overline{d}) = \overline{e}$, $\overline{e_i} = [F(\overline{c_i}), F(\overline{d_i})]$ (with common randomness for $i = 1, 2$)

Contents

- Introduction
- Idea for Homomorphic Operation
- Towards Secure Instantiation

- **Fact** [Dixon '08] For finite group H and sufficiently large L (depending only on $|H|$), for uniformly random $(x_i)_{i=1}^{L}$ except neg. prob., $\prod_{i=1}^{L}(x_i \text{ or } 1)$ is statistically close to uniform
- Sample_G and Sample_N are constructed from sufficiently many random elements of G and N

Candidate Strategy for Instantiation

1. Choose $\overline{G}$ and N with short group presentations
   - Yielding short presentation for $N \times \overline{G}$
2. Define $G = N \times \overline{G}$, with projection $\varphi \colon G \twoheadrightarrow \overline{G}$

Candidate Strategy for Instantiation

1. Choose $\overline{G}$ and N with short group presentations
   - Yielding short presentation for $N \times \overline{G}$
2. Define $G = N \times \overline{G}$, with projection $\varphi \colon G \twoheadrightarrow \overline{G}$
3. "Obfuscate" presentation for G by random iteration of Tietze transformations
   - sk is the record of transformations,
   - or generators of $\overline{G}$, to check whether $g \in N$

1. Choose $\overline{G}$ and N with short group presentations
   - Yielding short presentation for $N \times \overline{G}$
2. Define $G = N \times \overline{G}$, with projection $\varphi \colon G \twoheadrightarrow \overline{G}$
3. "Obfuscate" presentation for G by random iteration of Tietze transformations
   - sk is the record of transformations,
   - or generators of $\overline{G}$, to check whether $g \in N$
4. (Apply Knuth–Bendix Completion Algorithm to yield efficient group operation in obfuscated G)

- Determines a group (up to isomorphism) by generators and their fundamental relations
- Examples:
  - $\mathbb{Z}/n\mathbb{Z} = \langle x \mid x^n = 1 \rangle$
  - $\mathbb{Z}/15\mathbb{Z} = \langle x, y \mid x^3 = y^5 = [x, y] = 1 \rangle$
  - $S_4 = \langle s_1, s_2, s_3 \mid {s_1}^2 = {s_2}^2 = {s_3}^2 = (s_1 s_2)^3 = (s_2 s_3)^3 = (s_1 s_3)^2 = 1 \rangle$

Group Presentation

- Determines a group (up to isomorphism) by generators and their fundamental relations
- Examples:
  - $\mathbb{Z}/n\mathbb{Z} = \langle x \mid x^n = 1 \rangle$
  - $\mathbb{Z}/15\mathbb{Z} = \langle x, y \mid x^3 = y^5 = [x, y] = 1 \rangle$
  - $S_4 = \langle s_1, s_2, s_3 \mid {s_1}^2 = {s_2}^2 = {s_3}^2 = (s_1 s_2)^3 = (s_2 s_3)^3 = (s_1 s_3)^2 = 1 \rangle$
- **Fact** [Guralnick et al. '08] $\mathrm{SL}_2(\mathbb{F}_q)$ and some finite simple groups have short presentations (length $O(\log q)$ for $\mathrm{SL}_2(\mathbb{F}_q)$, q prime)

Tietze Transformation

- Changes presentation, keeping the group unchanged (up to isomorphism)
  - Add an already satisfied relation
  - Remove a redundant relation
  - Add a new generator expressed by old generators
  - Remove a generator which can be expressed by other generators

Example of Tietze Transformation

1. Start from $\langle x, y \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1 \rangle$

Example of Tietze Transformation

1. Start from $\langle x, y \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1 \rangle$
2. $\langle x, y, z \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1\,,\ z = xy \rangle$

Example of Tietze Transformation

1. Start from $\langle x, y \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1 \rangle$
2. $\langle x, y, z \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1\,,\ z = xy \rangle$
3. $\langle x, y, z \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1\,,\ x = zy^{-1} \rangle$

Example of Tietze Transformation

1. Start from $\langle x, y \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1 \rangle$
2. $\langle x, y, z \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1\,,\ z = xy \rangle$
3. $\langle x, y, z \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1\,,\ x = zy^{-1} \rangle$
4. $\langle y, z \mid (zy^{-1})^3 = y^5 = zyz^{-1}y^{-1} = 1 \rangle$

Example of Tietze Transformation

1. Start from $\langle x, y \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1 \rangle$
2. $\langle x, y, z \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1\,,\ z = xy \rangle$
3. $\langle x, y, z \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1\,,\ x = zy^{-1} \rangle$
4. $\langle y, z \mid (zy^{-1})^3 = y^5 = zyz^{-1}y^{-1} = 1 \rangle$
5. $\langle y, z \mid (zy^{-1})^3 = z^3y^{-3} = y^5 = zyz^{-1}y^{-1} = 1 \rangle$

Example of Tietze Transformation

1. Start from $\langle x, y \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1 \rangle$
2. $\langle x, y, z \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1\,,\ z = xy \rangle$
3. $\langle x, y, z \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1\,,\ x = zy^{-1} \rangle$
4. $\langle y, z \mid (zy^{-1})^3 = y^5 = zyz^{-1}y^{-1} = 1 \rangle$
5. $\langle y, z \mid (zy^{-1})^3 = z^3y^{-3} = y^5 = zyz^{-1}y^{-1} = 1 \rangle$
6. $\langle y, z \mid z^3y^{-3} = y^5 = zyz^{-1}y^{-1} = 1 \rangle$

Example of Tietze Transformation

1. Start from $\langle x, y \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1 \rangle$
2. $\langle x, y, z \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1\,,\ z = xy \rangle$
3. $\langle x, y, z \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1\,,\ x = zy^{-1} \rangle$
4. $\langle y, z \mid (zy^{-1})^3 = y^5 = zyz^{-1}y^{-1} = 1 \rangle$
5. $\langle y, z \mid (zy^{-1})^3 = z^3y^{-3} = y^5 = zyz^{-1}y^{-1} = 1 \rangle$
6. $\langle y, z \mid z^3y^{-3} = y^5 = zyz^{-1}y^{-1} = 1 \rangle$
7. $\langle y, z \mid z^3y^{-3} = y^5 = zyz^{-1}y^{-1} = 1\,,\ y = z^6 \rangle$

Example of Tietze Transformation

1. Start from $\langle x, y \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1 \rangle$
2. $\langle x, y, z \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1\,,\ z = xy \rangle$
3. $\langle x, y, z \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1\,,\ x = zy^{-1} \rangle$
4. $\langle y, z \mid (zy^{-1})^3 = y^5 = zyz^{-1}y^{-1} = 1 \rangle$
5. $\langle y, z \mid (zy^{-1})^3 = z^3y^{-3} = y^5 = zyz^{-1}y^{-1} = 1 \rangle$
6. $\langle y, z \mid z^3y^{-3} = y^5 = zyz^{-1}y^{-1} = 1 \rangle$
7. $\langle y, z \mid z^3y^{-3} = y^5 = zyz^{-1}y^{-1} = 1\,,\ y = z^6 \rangle$
8. $\langle z \mid z^3z^{-18} = z^{30} = zz^6z^{-1}z^{-6} = 1 \rangle$

Example of Tietze Transformation

1. Start from $\langle x, y \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1 \rangle$
2. $\langle x, y, z \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1\,,\ z = xy \rangle$
3. $\langle x, y, z \mid x^3 = y^5 = xyx^{-1}y^{-1} = 1\,,\ x = zy^{-1} \rangle$
4. $\langle y, z \mid (zy^{-1})^3 = y^5 = zyz^{-1}y^{-1} = 1 \rangle$
5. $\langle y, z \mid (zy^{-1})^3 = z^3y^{-3} = y^5 = zyz^{-1}y^{-1} = 1 \rangle$
6. $\langle y, z \mid z^3y^{-3} = y^5 = zyz^{-1}y^{-1} = 1 \rangle$
7. $\langle y, z \mid z^3y^{-3} = y^5 = zyz^{-1}y^{-1} = 1\,,\ y = z^6 \rangle$
8. $\langle z \mid z^3z^{-18} = z^{30} = zz^6z^{-1}z^{-6} = 1 \rangle$
9. $\langle z \mid z^{15} = 1 \rangle$ (This process is reversible)

Necessary Conditions for Groups

- If $g = (g_1, g_2), h = (h_1, h_2) \in G = N \times \overline{G}$, $g \neq h$ and $g_1 = h_1$, then $1 \neq g^{-1}h \in \overline{G}$, a part of trapdoor information
  - By birthday paradox, $\sqrt{|N|}$ must be large

Necessary Conditions for Groups

- If $g = (g_1, g_2), h = (h_1, h_2) \in G = N \times \overline{G}$, $g \neq h$ and $g_1 = h_1$, then $1 \neq g^{-1}h \in \overline{G}$, a part of trapdoor information
    - By birthday paradox, $\sqrt{|N|}$ must be large
- "Equations" in N satisfied with high prob. (but not in $\overline{G}$) can distinguish $c_2 \in N$ and $c_2 \in G$
    - If N commutative, $xy = yx$ with prob. 1
    - If $N = A_p$ (p prime), $x^p = 1$ with prob. $2/p$
    - Hence these groups cannot be used

Candidate Choice of Groups

- In $\mathrm{SL}_2(\mathbb{F}_q)$ (q prime), $\Pr[\mathrm{ord}(x) = k] \leq \mathrm{neg.}$ unless $k \mid q \pm 1$ and $k \approx q$ or $k = q$
  - Such k would be difficult to find, if q is hidden (by Tietze transformations)

Candidate Choice of Groups

- In $\mathrm{SL}_2(\mathbb{F}_q)$ (q prime), $\Pr[\mathrm{ord}(x) = k] \leq \mathrm{neg.}$ unless $k \mid q \pm 1$ and $k \approx q$ or $k = q$
  - Such k would be difficult to find, if q is hidden (by Tietze transformations)
- $N = \mathrm{SL}_2(\mathbb{F}_q)$, $\overline{G} = \mathrm{SL}_2(\mathbb{F}_{q'})$ would be good
  - Or N being simple groups of Lie type (or their semidirect products)?

Candidate Choice of Groups

- In $\mathrm{SL}_2(\mathbb{F}_q)$ (q prime), $\Pr[\mathrm{ord}(x) = k] \leq \mathrm{neg.}$ unless $k \mid q \pm 1$ and $k \approx q$ or $k = q$
  - Such k would be difficult to find, if q is hidden (by Tietze transformations)
- $N = \mathrm{SL}_2(\mathbb{F}_q)$, $\overline{G} = \mathrm{SL}_2(\mathbb{F}_{q'})$ would be good
  - Or N being simple groups of Lie type (or their semidirect products)?
- **Problem:** "Non-artificial" construction? (without group presentations)

- [Ostrovsky–Skeith III CRYPTO'08]: HE with **non-commutative simple group** as plaintext space implies FHE without bootstrapping
- The strategy based on Tietze transformation would be applicable to realize it as well

Summary of Talk

- Proposal of FHE without bootstrapping, based on non-commutative groups (ePrint 2014/097)
  - Homomorphic operators from commutator with rerandomized inputs
  - Constructing underlying groups by group presentations (generators and their relations)
  - "Obfuscating" group structure by random transformations of group presentation
- Candidate choice of groups
  - Attacks for inappropriate groups