Fully Homomorphic Encryption: A Holy Grail of Cryptography

Student: Jakub Klemsa,
Supervisor: Valtteri Niemi

Department of Computer Science,
University of Helsinki

November 21, 2015
1. Introduction to FHE
   - Definition of FHE
   - Goal of FHE
   - History
   - Recent Advances

2. FHE Framework by Nuida
   - Introduction
   - Requirements
   - Proposal
   - Cryptanalysis
   - Future Work
Definition of FHE

Definition (Fully Homomorphic Encryption)

FHE is a public key encryption scheme which consists of 4 poly-time algorithms (K, E, D, V) where

- given a security parameter $\lambda$, K outputs a keypair ($pk$, $sk$),
- given $pk$ and $m \in M$, E outputs randomized* encryption of $m$,
- given $sk$ and $c \in C$, an encryption of $m$, D outputs $m$,
- given $pk$, a function $f : M^t \to M$ and $(c_1, \ldots, c_t)$ encryptions of $(m_1, \ldots, m_t)$, V outputs $c$ which encrypts $f(m_1, \ldots, m_t)$.

*To achieve CPA security, public key scheme must be randomized.
Goal of FHE

- poly-time computation $\sim$ evaluation of a poly-time evaluable function
- computation with encrypted data!
- e.g. in cloud services
Goal of FHE

- poly-time computation \(\sim\) evaluation of a poly-time evaluable function
- **computation with encrypted data!**
- e.g. in cloud services
History

Example

RSA is homomorphic in $\mathbb{Z}/n\mathbb{Z}$ w.r.t. multiplication:

$$E(m_1 \cdot m_2) = (m_1 \cdot m_2)^e = m_1^e \cdot m_2^e = E(m_1) \cdot E(m_2).$$

- initial idea of FHE by Rivest, Adleman and Dertouzos [4] in 1978
- FHE not known to be even possible for decades
- first FHE by Gentry [1] in 2009
  - enormous computational overhead
Example

RSA is homomorphic in $\mathbb{Z}/n\mathbb{Z}$ w.r.t. multiplication:

$$E(m_1 \cdot m_2) = (m_1 \cdot m_2)^e = m_1^e \cdot m_2^e = E(m_1) \cdot E(m_2).$$

- initial idea of FHE by Rivest, Adleman and Dertouzos [4] in 1978
- FHE not known to be even possible for decades
- first FHE by Gentry [1] in 2009
  - enormous computational overhead
Recent Advances

- since Gentry’s breakthrough a very active research area
- proposed schemes often proved to be insecure
  - e.g. Liu [2] and Yagisawa [6], both disproved by Wang [5]
- promising framework by Nuida [3]
Introduction to Nuida’s FHE Framework

- operations AND and NOT instead
  - sufficient for any computation
- bits encoded into pairs \((x, y) \in G^2\) where \(y \neq 1_G, G\) group
  - \(0 \sim (1_G, y)\)
  - \(1 \sim (y, y)\)
- operations defined using commutator: 
  \[ [x, y] = x \cdot y \cdot x^{-1} \cdot y^{-1} \]
- underlying group \(G\) noncommutative!
Introduction to Nuida’s FHE Framework

- operations AND and NOT instead
  - sufficient for any computation
- bits encoded into pairs \((x, y) \in G^2\) where \(y \neq 1_G\), \(G\) group
  - \(0 \sim (1_G, y)\)
  - \(1 \sim (y, y)\)
- operations defined using commutator: \([x, y] = x \cdot y \cdot x^{-1} \cdot y^{-1}\)
- underlying group \(G\) noncommutative!
Definition of Operations

\[ y \neq 1_G \quad 0 \sim (1_G, y) \quad 1 \sim (y, y) \quad [x, y] = x \cdot y \cdot x^{-1} \cdot y^{-1} \]

- (\(x_1, y_1\)) AND (\(x_2, y_2\)) := ([x_1, x_2], [y_1, y_2])^{\dagger\ddagger}
  - if w.l.o.g. \((x_1, y_1) \sim 0\) i.e. \(x_1 = 1_G\)
    - then \([x_1, x_2] = 1_G\) i.e. \([x_1, x_2], [y_1, y_2]\) \sim 0
  - if \((x_1, y_1) \sim (x_2, y_2) \sim 1\) i.e. \(x_1 = y_1\) and \(x_2 = y_2\)
    - then \([x_1, x_2] = [y_1, y_2]\)
  - note that \([y_1, y_2] \neq 1_G\) i.e. \(y_1 \neq y_2\) and must not commute

\(^\dagger\) Originally \(([g x_1 g^{-1}, x_2], [g y_1 g^{-1}, y_2])\) where \(g\) is random. Not necessary.
\(^\ddagger\) Originally originally there was a typo.
Definition of Operations

\[ y \neq 1_G \quad 0 \sim (1_G, y) \quad 1 \sim (y, y) \quad [x, y] = x \cdot y \cdot x^{-1} \cdot y^{-1} \]

- \((x_1, y_1) \text{ AND } (x_2, y_2) := ([x_1, x_2], [y_1, y_2])^{\dagger\ddagger}\)
  - if w.l.o.g. \((x_1, y_1) \sim 0\) i.e. \(x_1 = 1_G\)
    then \([x_1, x_2] = 1_G\) i.e. \(([x_1, x_2], [y_1, y_2]) \sim 0\)
  - if \((x_1, y_1) \sim (x_2, y_2) \sim 1\) i.e. \(x_1 = y_1\) and \(x_2 = y_2\)
    then \([x_1, x_2] = [y_1, y_2] \uparrow \downarrow\)
    - note that \([y_1, y_2] \neq 1_G\) i.e. \(y_1 \neq y_2\) and must not commute

\text{\(\dagger\)Originally \(([gx_1g^{-1}, x_2], [gy_1g^{-1}, y_2])\) where \(g\) is random. Not necessary.}
\text{\(\ddagger\)Originally originally there was a typo.}
Definition of Operations

\[ y \neq 1_G \quad 0 \sim (1_G, y) \quad 1 \sim (y, y) \quad [x, y] = x \cdot y \cdot x^{-1} \cdot y^{-1} \]

- \( (x_1, y_1) \) AND \( (x_2, y_2) := ([x_1, x_2], [y_1, y_2])^{††} \)
  - if w.l.o.g. \( (x_1, y_1) \sim 0 \) i.e. \( x_1 = 1_G \)
    - then \( [x_1, x_2] = 1_G \) i.e. \( ([x_1, x_2], [y_1, y_2]) \sim 0 \)
  - if \( (x_1, y_1) \sim (x_2, y_2) \sim 1 \) i.e. \( x_1 = y_1 \) and \( x_2 = y_2 \)
    - then \( [x_1, x_2] = [y_1, y_2] \)

- note that \([y_1, y_2] \neq 1_G\) i.e. \( y_1 \neq y_2 \) and must not commute

\[\text{†Originally } ([gx_1g^{-1}, x_2], [gy_1g^{-1}, y_2]) \text{ where } g \text{ is random. Not necessary.}\]
\[\text{‡Originally originally there was a typo.}\]
Definition of Operations

\[ y \neq 1_G \quad 0 \sim (1_G, y) \quad 1 \sim (y, y) \quad [x, y] = x \cdot y \cdot x^{-1} \cdot y^{-1} \]

- NOT \( (x, y) := (x^{-1}y, y) \)
  - if \( (x, y) \sim 0 \) i.e. \( x = 1_G \)
    then \( x^{-1}y = y \) i.e. \( (x^{-1}y, y) \sim 1 \)
  - if \( (x, y) \sim 1 \) i.e. \( x = y \)
    then \( x^{-1}y = 1_G \) i.e. \( (x^{-1}y, y) \sim 0 \)
Definition of Operations

\[ y \neq 1_G \quad 0 \sim (1_G, y) \quad 1 \sim (y, y) \quad [x, y] = x \cdot y \cdot x^{-1} \cdot y^{-1} \]

- **NOT** \((x, y) := (x^{-1}y, y)\)
  - if \((x, y) \sim 0\) i.e. \(x = 1_G\)
    - then \(x^{-1}y = y\) i.e. \((x^{-1}y, y) \sim 1\)
  - if \((x, y) \sim 1\) i.e. \(x = y\)
    - then \(x^{-1}y = 1_G\) i.e. \((x^{-1}y, y) \sim 0\)
Definition of Operations

\[ y \neq 1_G \quad 0 \sim (1_G, y) \quad 1 \sim (y, y) \quad [x, y] = x \cdot y \cdot x^{-1} \cdot y^{-1} \]

- **NOT** \((x, y) := (x^{-1}y, y)\)
  - if \((x, y) \sim 0\) i.e. \(x = 1_G\), then \(x^{-1}y = y\) i.e. \((x^{-1}y, y) \sim 1\)
  - if \((x, y) \sim 1\) i.e. \(x = y\), then \(x^{-1}y = 1_G\) i.e. \((x^{-1}y, y) \sim 0\)
Encryption, Decryption – Most General Setup

- $H = \ker(\varphi)$

- sofar only encoding, needs encryption s.t. decryption is
  - homomorphic – to preserve operations, and
  - surjective with secret nontriv. kernel – randomization

- let $\varphi : \bar{G} \to G$ be such homomorphism

Student: Jakub Klemsa, Supervisor: Valtteri Niemi
Encryption, Decryption – Most General Setup

Key generation
- \( pk = (h_1, \ldots, h_t, g_1, \ldots, g_u) \in \ker(\varphi)^t \times \bar{G}^u \)
- \( sk \) – a decisional algorithm \( g \in \ker(\varphi) \)

Encryption
- \( h \in \ker(\varphi) \) – a random product of \( (h_1, \ldots, h_t) \), and \( g \in \bar{G} \) – a random product of \( (g_1, \ldots, g_u) \)
- \( E(0) = (h, g) \)
- \( E(1) = (gh, g) \)

Decryption
- \( D(x, y) = x \notin \ker(\varphi) \) using \( sk \)

Kernel distinguishability is hard \( \Rightarrow \) this scheme is secure.
Encryption, Decryption – Most General Setup

Key generation
- $pk = (h_1, \ldots, h_t, g_1, \ldots, g_u) \in \ker(\varphi)^t \times \bar{G}^u$
- $sk$ – a decisional algorithm $g \in \ker(\varphi)$

Encryption
- $h \in \ker(\varphi)$ – a random product of $(h_1, \ldots, h_t)$, and $g \in \bar{G}$ – a random product of $(g_1, \ldots, g_u)$
- $E(0) = (h, g)$
- $E(1) = (gh, g)$

Decryption
- $D(x, y) = x \not\in \ker(\varphi)$ using $sk$

Kernel distinguishability is hard $\Rightarrow$ this scheme is secure.
Encryption, Decryption – Most General Setup

Key generation
- \( pk = (h_1, \ldots, h_t, g_1, \ldots, g_u) \in \ker(\varphi)^t \times \bar{G}^u \)
- \( sk \) – a decisional algorithm \( g \tilde{\in} \ker(\varphi) \)

Encryption
- \( h \in \ker(\varphi) \) – a random product of \((h_1, \ldots, h_t)\), and 
- \( g \in \bar{G} \) – a random product of \((g_1, \ldots, g_u)\)
- \( E(0) = (h, g) \)
- \( E(1) = (gh, g) \)

Decryption
- \( D(x, y) = x \tilde{\in} \ker(\varphi) \) using \( sk \)

Kernel distinguishability is hard \( \Rightarrow \) this scheme is secure.
Encryption, Decryption – Most General Setup

Key generation
- \( pk = (h_1, \ldots, h_t, g_1, \ldots, g_u) \in \ker(\varphi)^t \times \bar{G}^u \)
- \( sk \) – a decisional algorithm \( g \in \ker(\varphi) \)

Encryption
- \( h \in \ker(\varphi) \) – a random product of \( (h_1, \ldots, h_t) \), and \( g \in \bar{G} \) – a random product of \( (g_1, \ldots, g_u) \)
- \( E(0) = (h, g) \)
- \( E(1) = (gh, g) \)

Decryption
- \( D(x, y) = x \notin \ker(\varphi) \) using \( sk \)

Kernel distinguishability is hard \( \Rightarrow \) this scheme is secure.
Nuida’s Suggestion – General Setup

Hiding kernel with trapdoor

- let $\varphi : \tilde{G} \rightarrow G$ be a known surjective homomorphism
- take $\tilde{G} > \tilde{G}$ and an (inner) automorphism $\tau : \tilde{G} \rightarrow \tilde{G}$
  - i.e. conjugation by a secret $t \in \tilde{G} \setminus \tilde{G}$
  - $\tau(\tilde{g}) = t^{-1}\tilde{g}t$
- $\varphi : (\tilde{G}) \rightarrow G$, $\varphi := \varphi \circ \tau$
  - $\ker(\varphi) = \tau^{-1}(\ker(\varphi)) = t \ker(\varphi)t^{-1}$

Summary

- $g \in G$ – encoding
- $\tilde{g} \in \tilde{G}$ – randomization
- $\tilde{\tilde{g}} \in \tau^{-1}(\tilde{G}) < \tilde{G}$ – encryption
Nuida’s Suggestion – General Setup

Hiding kernel with trapdoor

- let $\bar{\varphi} : \bar{G} \rightarrow G$ be a known surjective homomorphism
- take $\tilde{G} > \bar{G}$ and an (inner) automorphism $\tau : \tilde{G} \rightarrow \tilde{G}$
  - i.e. conjugation by a secret $t \in \tilde{G} \setminus \bar{G}$
  - $\tau(\tilde{g}) = t^{-1}\tilde{g}t$
- $\varphi : (\tilde{G}) \rightarrow G$, $\varphi := \bar{\varphi} \circ \tau$
  - $\ker(\varphi) = \tau^{-1}(\ker(\bar{\varphi})) = t \ker(\bar{\varphi}) t^{-1}$

Summary

- $g \in G$ – encoding
- $\bar{g} \in \bar{G}$ – randomization
- $\tilde{g} \in \tau^{-1}(\bar{G}) < \tilde{G}$ – encryption
Nuida’s Suggestion – General Setup

Hiding kernel with trapdoor

- Let $\overline{\varphi}: \tilde{G} \rightarrow G$ be a known surjective homomorphism
- Take $\tilde{G} > \tilde{G}$ and an (inner) automorphism $\tau: \tilde{G} \rightarrow \tilde{G}$
  - i.e. conjugation by a secret $t \in \tilde{G} \setminus \tilde{G}$
  - $\tau(\tilde{g}) = t^{-1}\tilde{g}t$
- $\varphi: (\tilde{G}) \rightarrow G$, $\varphi := \overline{\varphi} \circ \tau$
  - $\ker(\varphi) = \tau^{-1}(\ker(\overline{\varphi})) = t \ker(\overline{\varphi})t^{-1}$

Summary

- $g \in G$ – encoding
- $\tilde{g} \in \tilde{G}$ – randomization
- $\tilde{g} \in \tau^{-1}(\tilde{G}) < \tilde{G}$ – encryption
Nuida’s Suggestion – General Setup

Hiding kernel with trapdoor

- let $\bar{\varphi} : \bar{G} \rightarrow G$ be a known surjective homomorphism
- take $\tilde{G} > \bar{G}$ and an (inner) automorphism $\tau : \tilde{G} \rightarrow \tilde{G}$
  - i.e. conjugation by a secret $t \in \tilde{G} \setminus \bar{G}$
  - $\tau(\tilde{g}) = t^{-1}\tilde{g}t$
- $\varphi : (\tilde{G}) \rightarrow G$, $\varphi := \bar{\varphi} \circ \tau$
- $\ker(\varphi) = \tau^{-1}(\ker(\bar{\varphi})) = t \ker(\bar{\varphi}) t^{-1}$

Summary

- $g \in G$ – encoding
- $\bar{g} \in \bar{G}$ – randomization
- $\tilde{g} \in \tau^{-1}(\tilde{G}) < \tilde{G}$ – encryption
Nuida’s Suggestion – General Setup

Hiding kernel with trapdoor
- let $\bar{\phi} : \bar{G} \rightarrow G$ be a known surjective homomorphism
- take $\tilde{G} > \bar{G}$ and an (inner) automorphism $\tau : \tilde{G} \rightarrow \tilde{G}$
  - i.e. conjugation by a secret $t \in \tilde{G} \setminus \bar{G}$
  - $\tau(\tilde{g}) = t^{-1}\tilde{g}t$
- $\varphi : (\tilde{G}) \rightarrow G$, $\varphi := \bar{\phi} \circ \tau$
  - $\ker(\varphi) = \tau^{-1}(\ker(\bar{\phi})) = t\ker(\bar{\phi})t^{-1}$

Summary
- $g \in G$ – encoding
- $\bar{g} \in \bar{G}$ – randomization
- $\tilde{g} \in \tau^{-1}(\tilde{G}) < \tilde{G}$ – encryption
Nuida’s Suggestion – General Setup

Hiding kernel with trapdoor

- Let $\bar{\varphi} : \tilde{G} \rightarrow G$ be a known surjective homomorphism.
- Take $\tilde{G} > \bar{G}$ and an (inner) automorphism $\tau : \tilde{G} \rightarrow \tilde{G}$.
  - i.e. conjugation by a secret $t \in \tilde{G} \setminus \bar{G}$
  - $\tau(\tilde{g}) = t^{-1}\tilde{g}t$
- $\varphi : (\tilde{G}) \rightarrow G$, $\varphi := \bar{\varphi} \circ \tau$
  - $\ker(\varphi) = \tau^{-1}(\ker(\bar{\varphi})) = t \ker(\bar{\varphi})t^{-1}$

Summary

- $g \in G$ – encoding
- $\bar{g} \in \bar{G}$ – randomization
- $\tilde{g} \in \tau^{-1}(\bar{G}) < \tilde{G}$ – encryption
What properties do we need?

$H = \ker(\bar{\varphi})$, \hspace{1cm} \varphi = \bar{\varphi} \circ \tau$
Required Properties of General Setup

\[
H = \ker(\bar{\varphi}), \quad \varphi = \bar{\varphi} \circ \tau
\]

- \( \ker(\bar{\varphi}) = H \triangleleft \bar{G} \triangleleft \tilde{G} \)
  \Rightarrow \( \bar{G} \) shall have a nontrivial normal subgroup
  - way to achieve: \( G = K \times H \)
  - (construct \( \bar{\varphi} \) using \( H \) and 1st homomorphism theorem)
- AND gives \( ([x_1, x_2], [y_1, y_2]) \) i.e. moves to commutator subgroup
  \Rightarrow \( \tilde{G} \) shall be perfect (\( \tilde{G} \) equals to its commutator subgroup)
Required Properties of General Setup

\[ H = \ker(\bar{\varphi}), \quad \varphi = \bar{\varphi} \circ \tau \]

- \( \ker(\bar{\varphi}) = H \triangleleft \bar{G} \triangleleft \tilde{G} \)
- \( \Rightarrow \bar{G} \) shall have a nontrivial normal subgroup
  - way to achieve: \( G = K \times H \)
  - (construct \( \bar{\varphi} \) using \( H \) and 1st homomorphism theorem)
- AND gives \( ([x_1, x_2], [y_1, y_2]) \) i.e. moves to commutator subgroup
- \( \Rightarrow \tilde{G} \) shall be perfect (\( \tilde{G} \) equals to its commutator subgroup)
Introduction to FHE FHE Framework by Nuida References

Introduction Requirements Proposal Cryptanalysis Future Work

Required Properties of General Setup

\[
\begin{align*}
\tilde{G} & \cong G \\
H & = \text{ker}(\bar{\varphi}), \quad \varphi = \bar{\varphi} \circ \tau
\end{align*}
\]

- \(\text{ker}(\bar{\varphi}) = H \triangleleft \tilde{G} < \tilde{G}\)
  \(\Rightarrow\) \(\tilde{G}\) shall have a nontrivial normal subgroup
  - way to achieve: \(G = K \times H\)
  - (construct \(\bar{\varphi}\) using \(H\) and 1\(^{st}\) homomorphism theorem)

- AND gives \(([x_1, x_2], [y_1, y_2])\) i.e. moves to commutator subgroup
  \(\Rightarrow\) \(\tilde{G}\) shall be perfect (\(\tilde{G}\) equals to its commutator subgroup)

Student: Jakub Klemsa, Supervisor: Valtteri Niemi

Fully Homomorphic Encryption: A Holy Grail of Cryptography
Nuida mentioned special linear group $SL(2, \mathbb{F})$ – perfect group

$$SL(2, \mathbb{F}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{F}, \det(A) = 1 \right\}.$$
Proposal – Specific Setup

Put all together

- $H \triangleleft \tilde{G} \ldots \tilde{G} = K \times H$
- $\tilde{G}, H$ perfect ... $K, H = SL(2, \mathbb{F}), \tilde{G}$ perfect as well
- $\varphi$ with unknown kernel ... $\varphi = \bar{\varphi} \circ \tau$
  - $\bar{\varphi}$ known with nontrivial kernel $H$
  - $\tau$ automorphism ... inner automorphism i.e. $\tau(\tilde{g}) = t^{-1} \tilde{g} t$, $t$ secret

Note that

- $\tilde{G} = K \times H \simeq \left\{ \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} \bigg| A_{1,2} \in SL(2, \mathbb{F}) \right\}$, $\Theta = $ zero matrix
- $\bar{\varphi} \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} = A_1$, ker($\bar{\varphi}$) = $\left\{ \begin{pmatrix} I & \Theta \\ \Theta & A_2 \end{pmatrix} \bigg| A_2 \in SL(2, \mathbb{F}) \right\}$
- $\tilde{G} \leq \tilde{G} \ldots \tilde{G} = SL(4, \mathbb{F})$
Proposal – Specific Setup

Put all together

- \( H \triangleleft \tilde{G} \ldots \tilde{G} = K \times H \)
- \( \tilde{G}, H \) perfect \ldots \( K, H = SL(2, \mathbb{F}) \), \( \tilde{G} \) perfect as well
- \( \varphi \) with unknown kernel \ldots \( \varphi = \tilde{\varphi} \circ \tau \)
  - \( \tilde{\varphi} \) known with nontrivial kernel \( H \)
  - \( \tau \) automorphism \ldots \text{inner automorphism i.e. } \tau(\tilde{g}) = t^{-1}\tilde{g}t, t \text{ secret}

Note that

- \( \tilde{G} = K \times H \cong \left\{ \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} \middle| A_{1,2} \in SL(2, \mathbb{F}) \right\}, \Theta = \text{zero matrix} \)
- \( \tilde{\varphi} \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} = A_1, \text{ker}(\tilde{\varphi}) = \left\{ \begin{pmatrix} I & \Theta \\ \Theta & A_2 \end{pmatrix} \middle| A_2 \in SL(2, \mathbb{F}) \right\} \)
- \( \tilde{G} < \tilde{\tilde{G}} \ldots \tilde{\tilde{G}} = SL(4, \mathbb{F}) \)
Proposal – Specific Setup

Put all together

- $H \triangleleft \bar{G} \ldots \bar{G} = K \times H$
- $\bar{G}, H$ perfect $\ldots K, H = SL(2, F), \bar{G}$ perfect as well
- $\varphi$ with unknown kernel $\ldots \varphi = \bar{\varphi} \circ \tau$
  - $\bar{\varphi}$ known with nontrivial kernel $H$
  - $\tau$ automorphism $\ldots$ inner automorphism i.e. $\tau(\tilde{g}) = t^{-1}\tilde{g}t$, $t$ secret

Note that

- $\bar{G} = K \times H \simeq \left\{ \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} \Bigg| A_{1,2} \in SL(2, F) \right\}, \Theta = \text{zero matrix}$
- $\bar{\varphi} \begin{pmatrix} A_1 \\ \Theta \end{pmatrix} = A_1$, ker$(\bar{\varphi}) = \left\{ \begin{pmatrix} I & \Theta \\ \Theta & A_2 \end{pmatrix} \Bigg| A_2 \in SL(2, F) \right\}$
- $\bar{G} \triangleleft \tilde{G} \ldots \tilde{G} = SL(4, F)$
Proposal – Specific Setup

Put all together

- \( H \triangleleft \bar{G} \ldots \bar{G} = K \times H \)
- \( \bar{G}, H \) perfect \( \ldots K, H = SL(2, \mathbb{F}), \bar{G} \) perfect as well
- \( \varphi \) with unknown kernel \( \ldots \varphi = \bar{\varphi} \circ \tau \)
  - \( \bar{\varphi} \) known with nontrivial kernel \( H \)
  - \( \tau \) automorphism \( \ldots \) inner automorphism i.e. \( \tau(\tilde{g}) = t^{-1}\tilde{g}t, \ t \) secret

Note that

- \( \bar{G} = K \times H \cong \left\{ \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} \bigg| A_{1,2} \in SL(2, \mathbb{F}) \right\}, \Theta = \text{zero matrix} \)
- \( \bar{\varphi} \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} = A_1, \ker(\bar{\varphi}) = \left\{ \begin{pmatrix} I & \Theta \\ \Theta & A_2 \end{pmatrix} \bigg| A_2 \in SL(2, \mathbb{F}) \right\} \)
- \( \bar{G} < \bar{\bar{G}} \ldots \bar{G} = SL(4, \mathbb{F}) \)
Proposal – Specific Setup

Put all together

- $H \triangleleft \bar{G} \ldots \bar{G} = K \times H$
- $\bar{G}, H$ perfect $\ldots K, H = SL(2, \mathbb{F}), \bar{G}$ perfect as well
- $\varphi$ with unknown kernel $\ldots \varphi = \bar{\varphi} \circ \tau$
  - $\bar{\varphi}$ known with nontrivial kernel $H$
  - $\tau$ automorphism $\ldots$ inner automorphism i.e. $\tau(\tilde{g}) = t^{-1}\tilde{g}t$, $t$ secret

Note that

- $\bar{G} = K \times H \simeq \left\{ \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} \mid A_{1,2} \in SL(2, \mathbb{F}) \right\}$, $\Theta = \text{zero matrix}$
- $\bar{\varphi} \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} = A_1$, $\ker(\bar{\varphi}) = \left\{ \begin{pmatrix} I & \Theta \\ \Theta & A_2 \end{pmatrix} \mid A_2 \in SL(2, \mathbb{F}) \right\}$
- $\bar{G} < \tilde{G} \ldots \tilde{G} = SL(4, \mathbb{F})$
Proposal – Specific Setup

Put all together

- \( H \triangleleft \tilde{G} \ldots \tilde{G} = K \times H \)
- \( \tilde{G}, H \) perfect \ldots \( K, H = SL(2, \mathbb{F}) \), \( \tilde{G} \) perfect as well
- \( \varphi \) with unknown kernel \ldots \( \varphi = \bar{\varphi} \circ \tau \)
  - \( \bar{\varphi} \) known with nontrivial kernel \( H \)
  - \( \tau \) automorphism \ldots inner automorphism i.e. \( \tau(\tilde{g}) = t^{-1} \tilde{g} t \), \( t \) secret

Note that

- \( \tilde{G} = K \times H \simeq \left\{ \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} \Bigg| A_{1,2} \in SL(2, \mathbb{F}) \right\} , \Theta = \text{zero matrix} \)
- \( \bar{\varphi} \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} = A_1, \ker(\bar{\varphi}) = \left\{ \begin{pmatrix} I & \Theta \\ \Theta & A_2 \end{pmatrix} \Bigg| A_2 \in SL(2, \mathbb{F}) \right\} \)
- \( \tilde{G} < \tilde{G} \ldots \tilde{G} = SL(4, \mathbb{F}) \)
Cryptanalysis of Specific Setup

Does $\tau(M) := T^{-1}MT$ meet security requirements?
Cryptanalysis of Specific Setup

- problem to be hard: given $M \in \tau^{-1}(\tilde{G})$, decide $M \not\in \ker(\varphi) = \tau^{-1}(H) = THT^{-1}$

- such $M = T \begin{pmatrix} R & \Theta \\ \Theta & S \end{pmatrix} T^{-1}$ for some $R, S \in SL(2, \mathbb{F})$ and secret $T \in \tilde{G}$

- $\Rightarrow$ decide $R \not= I$

**Lemma**

There is an effective way to decide the previous decision problem without the knowledge of $T$ with overwhelming probability.
Cryptanalysis of Specific Setup

- problem to be hard: given $M \in \tau^{-1}(\tilde{G})$, decide
  $$M \notin \ker(\varphi) = \tau^{-1}(H) = THT^{-1}$$

- such $M = T \begin{pmatrix} R & \Theta \\ \Theta & S \end{pmatrix} T^{-1}$
  for some $R, S \in SL(2, \mathbb{F})$ and secret $T \in \tilde{G}$

- $\Rightarrow$ decide $R \neq I$

**Lemma**

*There is an effective way to decide the previous decision problem without the knowledge of $T$ with overwhelming probability.*
Cryptanalysis of Specific Setup

- problem to be hard: given \( M \in \tau^{-1}(\tilde{G}) \), decide
  \[
  M \overset{?}{\in} \ker(\varphi) = \tau^{-1}(H) = THT^{-1}
  \]
- such \( M = T \begin{pmatrix} R & \Theta \\ \Theta & S \end{pmatrix} T^{-1} \)
  for some \( R, S \in SL(2, \mathbb{F}) \) and secret \( T \in \tilde{G} \)
- \( \Rightarrow \) decide \( R \overset{?}{=} I \)

**Lemma**

There is an effective way to decide the previous decision problem without the knowledge of \( T \) with overwhelming probability.
Cryptanalysis of Specific Setup

- problem to be hard: given $M \in \tau^{-1}(\tilde{G})$, decide
  $M \not\in \ker(\varphi) = \tau^{-1}(H) = THT^{-1}$

- such $M = T \begin{pmatrix} R & \Theta \\ \Theta & S \end{pmatrix} T^{-1}$
  for some $R, S \in SL(2, \mathbb{F})$ and secret $T \in \tilde{G}$

- $\Rightarrow$ decide $R \not= I$

Lemma

There is an effective way to decide the previous decision problem without the knowledge of $T$ with overwhelming probability.
Cryptanalysis of Specific Setup

Lemma

There is an effective way to decide the previous decision problem without the knowledge of $T$ with overwhelming probability.

Proof.

Note that

$$M - I = T \begin{pmatrix} R & \Theta \\ \Theta & S \end{pmatrix} T^{-1} - TT^{-1} = T \begin{pmatrix} R - I & \Theta \\ \Theta & S - I \end{pmatrix} T^{-1}.$$ 

Here if $R = I$, then the resulting matrix $M - I$ has rank $\leq 2$. So if rank$(M - I) \leq 2$, then $R = I$ with overwhelming probability since $R, S$ are pseudorandom with determinant $= 1$. (The other options are $S = I$ or det$(R - I) = \det(S - I) = 0$, both negl.)
Cryptanalysis of Specific Setup

\[ \Rightarrow \text{testing } \text{rank}(M - I) ? \leq 2 \]

leads to plaintext recovery w.h.p.
### Possible Changes to Proposal

Put all together

- $H \triangleleft \tilde{G} \ldots \tilde{G} = K \times H$
- $	ilde{G}, H$ perfect ... $K, H = SL(2, \mathbb{F}), \tilde{G}$ perfect as well
- $\varphi$ with unknown kernel ... $\varphi = \bar{\varphi} \circ \tau$
  - $\bar{\varphi}$ known with nontrivial kernel $H$
  - $\tau$ automorphism ... inner automorphism i.e. $\tau(\tilde{g}) = t^{-1}\tilde{g}t$, $t$ secret

Note that

- $\tilde{G} = K \times H \simeq \left\{ \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} \bigg| A_{1,2} \in SL(2, \mathbb{F}) \right\}$, $\Theta =$ zero matrix

- $\bar{\varphi} \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} = A_1$, $\ker(\bar{\varphi}) = \left\{ \begin{pmatrix} I & \Theta \\ \Theta & A_2 \end{pmatrix} \bigg| A_2 \in SL(2, \mathbb{F}) \right\}$

- $\tilde{G} \leq \tilde{G} \ldots \tilde{G} = SL(4, \mathbb{F})$
Possible Changes to Proposal

Put all together

- $H \triangleleft \tilde{G} \ldots \tilde{G} = K \times H$
- $\tilde{G}, H$ perfect \ldots $K, H = SL(2, \mathbb{F}), \tilde{G}$ perfect as well
- $\varphi$ with unknown kernel \ldots $\varphi = \bar{\varphi} \circ \tau$
  - $\bar{\varphi}$ known with nontrivial kernel $H$
  - $\tau$ automorphism \ldots inner automorphism i.e. $\tau(\tilde{g}) = t^{-1}\tilde{g}t$, $t$ secret

Note that

- $\tilde{G} = K \times H \simeq \left\{ \left( \begin{array}{cc} A_1 & \Theta \\ \Theta & A_2 \end{array} \right) \bigg| A_{1,2} \in SL(2, \mathbb{F}) \right\}$, $\Theta = \text{zero matrix}$
- $\bar{\varphi} \left( \begin{array}{cc} A_1 & \Theta \\ \Theta & A_2 \end{array} \right) = A_1$, $\ker(\bar{\varphi}) = \left\{ \left( \begin{array}{cc} I & \Theta \\ \Theta & A_2 \end{array} \right) \bigg| A_2 \in SL(2, \mathbb{F}) \right\}$
- $\tilde{G} < \tilde{G} \ldots \tilde{G} = SL(4, \mathbb{F})$
Possible Changes to Proposal

Put all together

- $H \triangleleft \bar{G} \ldots \bar{G} = K \times H$
- $\bar{G}, H$ perfect $\ldots K, H = SL(2, \mathbb{F})$, $\bar{G}$ perfect as well
- $\varphi$ with unknown kernel $\ldots \varphi = \bar{\varphi} \circ \tau$
  - $\bar{\varphi}$ known with nontrivial kernel $H$
  - $\tau$ automorphism $\ldots$ inner automorphism i.e. $\tau(\tilde{g}) = t^{-1}\tilde{g}t$, $t$ secret

Note that

- $\bar{G} = K \times H \simeq \left\{ \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} \middle| A_{1,2} \in SL(2, \mathbb{F}) \right\}$, $\Theta = $ zero matrix

- $\bar{\varphi} \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} = A_1$, $\ker(\bar{\varphi}) = \left\{ \begin{pmatrix} I & \Theta \\ \Theta & A_2 \end{pmatrix} \middle| A_2 \in SL(2, \mathbb{F}) \right\}$

- $\bar{G} < \hat{G} \ldots \hat{G} = SL(4, \mathbb{F})$
Possible Changes to Proposal

Put all together

- \( H \triangleleft \bar{G} \ldots \bar{G} = K \times H \)
- \( \bar{G}, H \) perfect \ldots \( K, H = SL(2, \mathbb{F}) \), \( \bar{G} \) perfect as well
- \( \varphi \) with unknown kernel \ldots \( \varphi = \bar{\varphi} \circ \tau \)
  - \( \bar{\varphi} \) known with nontrivial kernel \( H \)
  - \( \tau \) automorphism \ldots inner automorphism i.e. \( \tau(\tilde{g}) = t^{-1}\tilde{g}t, t \) secret

Note that

- \( \bar{G} = K \times H \cong \left\{ \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} \bigg| A_{1,2} \in SL(2, \mathbb{F}) \right\}, \Theta = \text{zero matrix} \)
- \( \bar{\varphi} \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} = A_1, \ker(\bar{\varphi}) = \left\{ \begin{pmatrix} I & \Theta \\ \Theta & A_2 \end{pmatrix} \bigg| A_2 \in SL(2, \mathbb{F}) \right\} \)
- \( \bar{G} < \tilde{G} \ldots \tilde{G} = SL(4, \mathbb{F}) \)
Possible Changes to Proposal

Put all together

1. $H \triangleleft \bar{G} \ldots \bar{G} = K \times H$
2. $\bar{G}, H$ perfect ... $K, H = SL(2, \mathbb{F}), \bar{G}$ perfect as well
3. $\varphi$ with unknown kernel ... $\varphi = \bar{\varphi} \circ \tau$
   - $\bar{\varphi}$ known with nontrivial kernel $H$
   - $\tau$ automorphism ... inner automorphism i.e. $\tau(\tilde{g}) = t^{-1}\tilde{g}t$, $t$ secret

Note that

1. $\bar{G} = K \times H \simeq \left\{ \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} \bigg| A_{1,2} \in SL(2, \mathbb{F}) \right\}, \Theta = \text{zero matrix}$
2. $\bar{\varphi} \begin{pmatrix} A_1 & \Theta \\ \Theta & A_2 \end{pmatrix} = A_1$, $\ker(\bar{\varphi}) = \left\{ \begin{pmatrix} I & \Theta \\ \Theta & A_2 \end{pmatrix} \bigg| A_2 \in SL(2, \mathbb{F}) \right\}$
3. $\bar{G} < \tilde{G} \ldots \tilde{G} = SL(4, \mathbb{F})$
References

Craig Gentry et al.
Fully homomorphic encryption using ideal lattices.

Dongxi Liu.
Practical fully homomorphic encryption without noise reduction.

Koji Nuida.
A simple framework for noise-free construction of fully homomorphic encryption from a special class of non-commutative groups.
References II

