# Cryptanalysis of two matrix key establishment protocols

S.R. Blackburn, C. Cid, C. Mullan

Royal Holloway College, London

February 16, 2011

# Motivation: key establishment problem

- How do Alice and Bob securely establish a shared key?
- In practice, they can use the Diffie–Hellman protocol.
- But can we do any better? what about quantum adversaries? Efficiency? Diversity?
- Perhaps we can use matrix groups in some way...?

# Outline of talk

We will look at two schemes:

1. A symmetric key transport protocol by Baumslag, Camps, Fine, Rosenberger and Xu (BCFRX, 2006).

2. A public key agreement protocol by Habeeb, Kahrobaei and Shpilrain (HKS, 2010).

Both schemes suggest using matrix groups as a secure platform.

We provide a <u>concrete</u> description of each scheme, followed by a cryptanalysis in the passive adversary model.

# Before we start: some terminology

We will consider 2-party key establishment protocols. Some flavours:

- Key agreement protocol: key is a function of both parties.
- Key transport protocol: key is a function of just one party.
- public protocol: Alice and Bob do not share any secrets.
- symmetric protocol: Alice and Bob apriori share a secret.
  They wish to use it to establish a new session key.

# The BCFRX Scheme

- This is a symmetric key transport protocol.
- Various abstract platform groups proposed (e.g. $\mathrm{Aut}(F_n)$, surface braid groups)
- We consider their matrix group proposal: $\mathrm{SL}_4(\mathbb{Z})$.
- We describe (and cryptanalyse) the BCFRX protocol based on $\mathrm{SL}_4(\mathbb{Z})$.

# The BCFRX Scheme

- Loosely speaking, inside the BCFRX scheme over $\mathrm{SL}_4(\mathbb{Z})$ there are two simpler schemes, Scheme A and Scheme B:

$$\text{Scheme A} \subset \text{Scheme B} \subset \text{BCFRX Scheme.}$$

- We cryptanalyse Scheme A followed by Scheme B followed by the BCFRX scheme.

# The BCFRX Scheme

- Loosely speaking, inside the BCFRX scheme over $\mathrm{SL}_4(\mathbb{Z})$ there are two simpler schemes, Scheme A and Scheme B:

$$\text{Scheme A} \subset \text{Scheme B} \subset \text{BCFRX Scheme.}$$

- We cryptanalyse Scheme A followed by Scheme B followed by the BCFRX scheme.
- Scheme A is a public version of BCFRX over $\mathrm{SL}_4(p)$.
- Scheme B is a symmetric version of BCFRX over $\mathrm{SL}_4(p)$.
- Let's look at Scheme A..

# Scheme A description

- The scheme requires two commuting subgroups of $\mathrm{SL}_4(p)$.
- Alice samples the subgroup $\begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix}$.
- Bob samples the subgroup $\begin{pmatrix} I_2 & 0 \\ 0 & \mathrm{SL}_2(p) \end{pmatrix}$.
- These subgroups are known to an adversary.

# Scheme A description

- Flow 1: Bob picks a key $K \in \mathrm{SL}_4(p)$ and $S_{22}, S'_{22} \in \mathrm{SL}_2(p)$, and sends to Alice

$$C = \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} K \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix}.$$

# Scheme A description

- Flow 1: Bob picks a key $K \in \mathrm{SL}_4(p)$ and $S_{22}, S'_{22} \in \mathrm{SL}_2(p)$, and sends to Alice

$$C = \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} K \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix}.$$

- Flow 2: Alice picks $R_{11}, R'_{11} \in \mathrm{SL}_2(p)$ and replies

$$D = \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} C \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix}$$

# Scheme A description

- Flow 1: Bob picks a key $K \in \mathrm{SL}_4(p)$ and $S_{22}, S'_{22} \in \mathrm{SL}_2(p)$, and sends to Alice

$$C = \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} K \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix}.$$

- Flow 2: Alice picks $R_{11}, R'_{11} \in \mathrm{SL}_2(p)$ and replies

$$\begin{aligned} D &= \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} C \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} \\ &= \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} K \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} \end{aligned}$$

# Scheme A description

- Flow 1: Bob picks a key $K \in \mathrm{SL}_4(p)$ and $S_{22}, S'_{22} \in \mathrm{SL}_2(p)$, and sends to Alice

$$C = \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} K \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix}.$$

- Flow 2: Alice picks $R_{11}, R'_{11} \in \mathrm{SL}_2(p)$ and replies

$$\begin{aligned} D &= \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} C \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} \\ &= \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} K \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} \\ &= \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} K \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} \end{aligned}$$

# Scheme A description

- <u>Flow 3:</u> Bob replies

$$E = \begin{pmatrix} I_2 & 0 \\ 0 & S_{22}^{-1} \end{pmatrix} D \begin{pmatrix} I_2 & 0 \\ 0 & S'^{-1}_{22} \end{pmatrix}$$

# Scheme A description

- Flow 3: Bob replies

$$
\begin{aligned}
E &= \begin{pmatrix} I_2 & 0 \\ 0 & S_{22}^{-1} \end{pmatrix} D \begin{pmatrix} I_2 & 0 \\ 0 & {S'}_{22}^{-1} \end{pmatrix} \\
&= \begin{pmatrix} I_2 & 0 \\ 0 & S_{22}^{-1} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} K \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & {S'}_{22}^{-1} \end{pmatrix}
\end{aligned}
$$

# Scheme A description

- Flow 3: Bob replies

$$
\begin{aligned}
E &= \begin{pmatrix} I_2 & 0 \\ 0 & S_{22}^{-1} \end{pmatrix} D \begin{pmatrix} I_2 & 0 \\ 0 & {S'}_{22}^{-1} \end{pmatrix} \\
&= \begin{pmatrix} I_2 & 0 \\ 0 & S_{22}^{-1} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} K \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & {S'}_{22}^{-1} \end{pmatrix} \\
&= \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} K \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix}.
\end{aligned}
$$

# Scheme A description

- Flow 3: Bob replies

$$\begin{aligned} E &= \begin{pmatrix} I_2 & 0 \\ 0 & S_{22}^{-1} \end{pmatrix} D \begin{pmatrix} I_2 & 0 \\ 0 & {S'}_{22}^{-1} \end{pmatrix} \\ &= \begin{pmatrix} I_2 & 0 \\ 0 & S_{22}^{-1} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} K \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & {S'}_{22}^{-1} \end{pmatrix} \\ &= \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} K \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix}. \end{aligned}$$

- Alice computes

$$\begin{pmatrix} R_{11}^{-1} & 0 \\ 0 & I_2 \end{pmatrix} E \begin{pmatrix} {R'}_{11}^{-1} & 0 \\ 0 & I_2 \end{pmatrix}$$

# Scheme A description

- Flow 3: Bob replies

$$\begin{aligned} E &= \begin{pmatrix} I_2 & 0 \\ 0 & S_{22}^{-1} \end{pmatrix} D \begin{pmatrix} I_2 & 0 \\ 0 & {S'}_{22}^{-1} \end{pmatrix} \\ &= \begin{pmatrix} I_2 & 0 \\ 0 & S_{22}^{-1} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} K \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & {S'}_{22}^{-1} \end{pmatrix} \\ &= \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} K \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix}. \end{aligned}$$

- Alice computes

$$\begin{pmatrix} R_{11}^{-1} & 0 \\ 0 & I_2 \end{pmatrix} E \begin{pmatrix} {R'}_{11}^{-1} & 0 \\ 0 & I_2 \end{pmatrix} = \begin{pmatrix} R_{11}^{-1} & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} K \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} {R'}_{11}^{-1} & 0 \\ 0 & I_2 \end{pmatrix}$$

## Scheme A description

- <u>Flow 3:</u> Bob replies

$$\begin{aligned} E &= \begin{pmatrix} I_2 & 0 \\ 0 & S_{22}^{-1} \end{pmatrix} D \begin{pmatrix} I_2 & 0 \\ 0 & {S'}_{22}^{-1} \end{pmatrix} \\ &= \begin{pmatrix} I_2 & 0 \\ 0 & S_{22}^{-1} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} K \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & {S'}_{22}^{-1} \end{pmatrix} \\ &= \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} K \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix}. \end{aligned}$$

- Alice computes

$$\begin{aligned} \begin{pmatrix} R_{11}^{-1} & 0 \\ 0 & I_2 \end{pmatrix} E \begin{pmatrix} {R'}_{11}^{-1} & 0 \\ 0 & I_2 \end{pmatrix} &= \begin{pmatrix} R_{11}^{-1} & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} K \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} {R'}_{11}^{-1} & 0 \\ 0 & I_2 \end{pmatrix} \\ &= K. \end{aligned}$$

# Scheme A: a cryptanalysis

- Goal of passive adversary: to compute $K$ from the 3 transmitted matrices $C, D, E$.

- For a general $4 \times 4$ matrix $Z$, write $Z$ in block form as:

$$Z = \begin{pmatrix} Z_{11} & Z_{12} \\ Z_{21} & Z_{22} \end{pmatrix}.$$

# Scheme A: a cryptanalysis

- <u>Flow 1:</u> $C = \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} \begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix}$

# Scheme A: a cryptanalysis

- Flow 1: $C = \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} \begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12}S'_{22} \\ S_{22}K_{21} & S_{22}K_{22}S'_{22} \end{pmatrix}$.

# Scheme A: a cryptanalysis

- Flow 1: $C = \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} \begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12}S'_{22} \\ S_{22}K_{21} & S_{22}K_{22}S'_{22} \end{pmatrix}.$
- Flow 2: $D = \begin{pmatrix} R_{11}K_{11}R'_{11} & R_{11}K_{12}S'_{22} \\ S_{22}K_{21}R_{11} & S_{22}K'_{22}S'_{22} \end{pmatrix}.$

# Scheme A: a cryptanalysis

- <u>Flow 1:</u> $C = \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} \begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12}S'_{22} \\ S_{22}K_{21} & S_{22}K_{22}S'_{22} \end{pmatrix}$.
- <u>Flow 2:</u> $D = \begin{pmatrix} R_{11}K_{11}R'_{11} & R_{11}K_{12}S'_{22} \\ S_{22}K_{21}R_{11} & S_{22}K'_{22}S'_{22} \end{pmatrix}$.
- <u>Flow 3:</u> $E = \begin{pmatrix} R_{11}K_{11}R'_{11} & R_{11}K_{12} \\ K_{21}R_{11} & K_{22} \end{pmatrix}$.

# Scheme A: a cryptanalysis

- Flow 1: $C = \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} \begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12}S'_{22} \\ S_{22}K_{21} & S_{22}K_{22}S'_{22} \end{pmatrix}.$
- Flow 2: $D = \begin{pmatrix} R_{11}K_{11}R'_{11} & R_{11}K_{12}S'_{22} \\ S_{22}K_{21}R_{11} & S_{22}K'_{22}S'_{22} \end{pmatrix}.$
- Flow 3: $E = \begin{pmatrix} R_{11}K_{11}R'_{11} & R_{11}K_{12} \\ K_{21}R_{11} & K_{22} \end{pmatrix}.$ So Eve knows $K_{11}, K_{22}$.

# Scheme A: a cryptanalysis

- Flow 1: $C = \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} \begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12}S'_{22} \\ S_{22}K_{21} & S_{22}K_{22}S'_{22} \end{pmatrix}$.

- Flow 2: $D = \begin{pmatrix} R_{11}K_{11}R'_{11} & R_{11}K_{12}S'_{22} \\ S_{22}K_{21}R_{11} & S_{22}K'_{22}S'_{22} \end{pmatrix}$.

- Flow 3: $E = \begin{pmatrix} R_{11}K_{11}R'_{11} & R_{11}K_{12} \\ K_{21}R_{11} & K_{22} \end{pmatrix}$. So Eve knows $K_{11}, K_{22}$.

- To find $K_{12}$, we find $X$ such that $X(R_{11}K_{12}S'_{22}) = K_{12}S'_{22}$.

# Scheme A: a cryptanalysis

- Flow 1: $C = \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} \begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12}S'_{22} \\ S_{22}K_{21} & S_{22}K_{22}S'_{22} \end{pmatrix}$.
- Flow 2: $D = \begin{pmatrix} R_{11}K_{11}R'_{11} & R_{11}K_{12}S'_{22} \\ S_{22}K_{21}R_{11} & S_{22}K'_{22}S'_{22} \end{pmatrix}$.
- Flow 3: $E = \begin{pmatrix} R_{11}K_{11}R'_{11} & R_{11}K_{12} \\ K_{21}R_{11} & K_{22} \end{pmatrix}$. So Eve knows $K_{11}, K_{22}$.
- To find $K_{12}$, we find $X$ such that $X(R_{11}K_{12}S'_{22}) = K_{12}S'_{22}$.
- This implies $X(R_{11}K_{12}) = K_{12}$.

# Scheme A: a cryptanalysis

- Flow 1: $C = \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} \begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12}S'_{22} \\ S_{22}K_{21} & S_{22}K_{22}S'_{22} \end{pmatrix}$.
- Flow 2: $D = \begin{pmatrix} R_{11}K_{11}R'_{11} & R_{11}K_{12}S'_{22} \\ S_{22}K_{21}R_{11} & S_{22}K'_{22}S'_{22} \end{pmatrix}$.
- Flow 3: $E = \begin{pmatrix} R_{11}K_{11}R'_{11} & R_{11}K_{12} \\ K_{21}R_{11} & K_{22} \end{pmatrix}$. So Eve knows $K_{11}, K_{22}$.
- To find $K_{12}$, we find $X$ such that $X(R_{11}K_{12}S'_{22}) = K_{12}S'_{22}$.
- This implies $X(R_{11}K_{12}) = K_{12}$. So Eve knows $K_{12}$.

# Scheme A: a cryptanalysis

- <u>Flow 1:</u> $C = \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} \begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12}S'_{22} \\ S_{22}K_{21} & S_{22}K_{22}S'_{22} \end{pmatrix}$.

- <u>Flow 2:</u> $D = \begin{pmatrix} R_{11}K_{11}R'_{11} & R_{11}K_{12}S'_{22} \\ S_{22}K_{21}R_{11} & S_{22}K'_{22}S'_{22} \end{pmatrix}$.

- <u>Flow 3:</u> $E = \begin{pmatrix} R_{11}K_{11}R'_{11} & R_{11}K_{12} \\ K_{21}R_{11} & K_{22} \end{pmatrix}$. So Eve knows $K_{11}, K_{22}$.

- To find $K_{12}$, we find $X$ such that $X(R_{11}K_{12}S'_{22}) = K_{12}S'_{22}$.
- This implies $X(R_{11}K_{12}) = K_{12}$. So Eve knows $K_{12}$.

- Exercise: compute $K_{21}$.

# Scheme A: a cryptanalysis

- Flow 1: $C = \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} \begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12}S'_{22} \\ S_{22}K_{21} & S_{22}K_{22}S'_{22} \end{pmatrix}$.
- Flow 2: $D = \begin{pmatrix} R_{11}K_{11}R'_{11} & R_{11}K_{12}S'_{22} \\ S_{22}K_{21}R_{11} & S_{22}K'_{22}S'_{22} \end{pmatrix}$.
- Flow 3: $E = \begin{pmatrix} R_{11}K_{11}R'_{11} & R_{11}K_{12} \\ K_{21}R_{11} & K_{22} \end{pmatrix}$. So Eve knows $K_{11}, K_{22}$.
- To find $K_{12}$, we find $X$ such that $X(R_{11}K_{12}S'_{22}) = K_{12}S'_{22}$.
- This implies $X(R_{11}K_{12}) = K_{12}$. So Eve knows $K_{12}$.
- Exercise: compute $K_{21}$.
- So Eve can compute $K$ and Scheme A is broken.

# So far so good..

- Recall: Scheme A $\subset$ Scheme B $\subset$ BCFRX Scheme, where:
- Scheme A is a public version of BCFRX over $\mathrm{SL}_4(p)$.
- Scheme B is a symmetric version of BCFRX over $\mathrm{SL}_4(p)$.
- Let's look at Scheme B..

# Scheme B description

- Alice and Bob share a secret matrix $M \in \mathrm{SL}_4(p)$.

# Scheme B description

- Alice and Bob share a secret matrix $M \in \mathrm{SL}_4(p)$.
- We still require commuting subgroups of $\mathrm{SL}_4(p)$.
- Now Alice samples the subgroup $M^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} M$.
- And Bob samples the subgroup $M^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & \mathrm{SL}_2(p) \end{pmatrix} M$.

# Scheme B description

- Alice and Bob share a secret matrix $M \in \mathrm{SL}_4(p)$.
- We still require commuting subgroups of $\mathrm{SL}_4(p)$.
- Now Alice samples the subgroup $M^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} M$.
- And Bob samples the subgroup $M^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & \mathrm{SL}_2(p) \end{pmatrix} M$.
- An adversary does NOT know these subgroups.
- The rest of the protocol is exactly the same..

## Scheme B description

- Flow 1: Bob picks a key $K \in \mathrm{SL}_4(p)$ and $S_{22}, S'_{22} \in \mathrm{SL}_2(p)$, and sends to Alice

$$C = M^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} MKM^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} M.$$

# Scheme B description

- <u>Flow 1:</u> Bob picks a key $K \in \mathrm{SL}_4(p)$ and $S_{22}, S'_{22} \in \mathrm{SL}_2(p)$, and sends to Alice

$$C = M^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} MKM^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} M.$$

- <u>Flow 2:</u> Alice picks $R_{11}, R'_{11} \in \mathrm{SL}_2(p)$ and replies

$$D = M^{-1} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} MCM^{-1} \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} M$$

# Scheme B description

- <u>Flow 1:</u> Bob picks a key $K \in \mathrm{SL}_4(p)$ and $S_{22}, S'_{22} \in \mathrm{SL}_2(p)$, and sends to Alice

$$C = M^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} MKM^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} M.$$

- <u>Flow 2:</u> Alice picks $R_{11}, R'_{11} \in \mathrm{SL}_2(p)$ and replies

$$\begin{aligned} D &= M^{-1} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} MCM^{-1} \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} M \\ &= M^{-1} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} MM^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} MKM^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} MM^{-1} \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} M \end{aligned}$$

# Scheme B description

- <u>Flow 1:</u> Bob picks a key $K \in \mathrm{SL}_4(p)$ and $S_{22}, S'_{22} \in \mathrm{SL}_2(p)$, and sends to Alice

$$C = M^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} MKM^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} M.$$

- <u>Flow 2:</u> Alice picks $R_{11}, R'_{11} \in \mathrm{SL}_2(p)$ and replies

$$\begin{aligned} D &= M^{-1} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} MCM^{-1} \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} M \\ &= M^{-1} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} MM^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} MKM^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} MM^{-1} \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} M \\ &= M^{-1} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} MKM^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} M \end{aligned}$$

# Scheme B description

- Flow 1: Bob picks a key $K \in \mathrm{SL}_4(p)$ and $S_{22}, S'_{22} \in \mathrm{SL}_2(p)$, and sends to Alice

$$C = M^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} MKM^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} M.$$

- Flow 2: Alice picks $R_{11}, R'_{11} \in \mathrm{SL}_2(p)$ and replies

$$\begin{aligned}
D &= M^{-1} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} MCM^{-1} \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} M \\
&= M^{-1} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} MM^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} MKM^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} MM^{-1} \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} M \\
&= M^{-1} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} MKM^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} M \\
&= M^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22} \end{pmatrix} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} MKM^{-1} \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ 0 & S'_{22} \end{pmatrix} M
\end{aligned}$$

# Scheme B description

- Flow 3: Bob replies

$$E = M^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22}^{-1} \end{pmatrix} MDM^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & {S'}_{22}^{-1} \end{pmatrix} M$$

# Scheme B description

- <u>Flow 3:</u> Bob replies

$$
\begin{aligned}
E &= M^{-1}\begin{pmatrix} I_2 & 0 \\ 0 & S_{22}^{-1} \end{pmatrix} MDM^{-1}\begin{pmatrix} I_2 & 0 \\ 0 & {S'}_{22}^{-1} \end{pmatrix} M \\
&= M^{-1}\begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} MKM^{-1}\begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} M.
\end{aligned}
$$

# Scheme B description

- Flow 3: Bob replies

$$\begin{aligned} E &= M^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & S_{22}^{-1} \end{pmatrix} MDM^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & {S'}_{22}^{-1} \end{pmatrix} M \\ &= M^{-1} \begin{pmatrix} R_{11} & 0 \\ 0 & I_2 \end{pmatrix} MKM^{-1} \begin{pmatrix} R'_{11} & 0 \\ 0 & I_2 \end{pmatrix} M. \end{aligned}$$

- Since Alice knows $R_{11}, R'_{11}$ and $M$, she can compute $K$.

# Scheme B cryptanalysis

- Alice samples the subgroup $\mathcal{A} = M^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} M$.

- Bob samples the subgroup $\mathcal{B} = M^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & \mathrm{SL}_2(p) \end{pmatrix} M$.

# Scheme B cryptanalysis

- Alice samples the subgroup $\mathcal{A} = M^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} M$.

- Bob samples the subgroup $\mathcal{B} = M^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & \mathrm{SL}_2(p) \end{pmatrix} M$.

- If Eve knows $M$ we are in Scheme $A$.

# Scheme B cryptanalysis

- Alice samples the subgroup $\mathcal{A} = M^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} M$.
- Bob samples the subgroup $\mathcal{B} = M^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & \mathrm{SL}_2(p) \end{pmatrix} M$.
- If Eve knows $M$ we are in Scheme $A$.
- So to break Scheme $B$ it suffices to find $M$.

# Scheme B cryptanalysis

- Alice samples the subgroup $\mathcal{A} = M^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} M$.
- Bob samples the subgroup $\mathcal{B} = M^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & \mathrm{SL}_2(p) \end{pmatrix} M$.
- If Eve knows $M$ we are in Scheme $A$.
- So to break Scheme $B$ it suffices to find $M$.
  But it's not necessary to find $M$!

# Scheme B cryptanalysis

- Alice samples the subgroup $\mathcal{A} = M^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} M$.
- Bob samples the subgroup $\mathcal{B} = M^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & \mathrm{SL}_2(p) \end{pmatrix} M$.
- If Eve knows $M$ we are in Scheme $A$.
- So to break Scheme $B$ it suffices to find $M$.
  But it's not necessary to find $M$!
- We just need to find any invertible matrix $N$ such that:

$$\mathcal{A} = N^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} N, \quad \mathcal{B} = N^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & \mathrm{SL}_2(p) \end{pmatrix} N.$$

# Scheme B cryptanalysis

## Lemma

Eve can compute $K$ if she knows a matrix $N$ such that

$$\mathcal{A} = N^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} N, \quad \mathcal{B} = N^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & \mathrm{SL}_2(p) \end{pmatrix} N.$$

# Scheme B cryptanalysis

## Lemma

Eve can compute $K$ if she knows a matrix $N$ such that

$$\mathcal{A} = N^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} N, \quad \mathcal{B} = N^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & \mathrm{SL}_2(p) \end{pmatrix} N.$$

## Proof

- Suppose Eve knows $N$.

# Scheme B cryptanalysis

## Lemma

Eve can compute $K$ if she knows a matrix $N$ such that

$$\mathcal{A} = N^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} N, \quad \mathcal{B} = N^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & \mathrm{SL}_2(p) \end{pmatrix} N.$$

## Proof

- Suppose Eve knows $N$.
- Given transmitted matrices $C, D, E$, conjugate by $N$: $NCN^{-1}, NDN^{-1}, NEN^{-1}$.

# Scheme B cryptanalysis

## Lemma

Eve can compute $K$ if she knows a matrix $N$ such that

$$\mathcal{A} = N^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} N, \quad \mathcal{B} = N^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & \mathrm{SL}_2(p) \end{pmatrix} N.$$

## Proof

- Suppose Eve knows $N$.
- Given transmitted matrices $C, D, E$, conjugate by $N$: $NCN^{-1}, NDN^{-1}, NEN^{-1}$.
- Use linear algebra to compute $NKN^{-1}$ (as we did for Scheme A).

# Scheme B cryptanalysis

## Lemma

Eve can compute $K$ if she knows a matrix $N$ such that

$$\mathcal{A} = N^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} N, \quad \mathcal{B} = N^{-1} \begin{pmatrix} I_2 & 0 \\ 0 & \mathrm{SL}_2(p) \end{pmatrix} N.$$

## Proof

- Suppose Eve knows $N$.
- Given transmitted matrices $C, D, E$, conjugate by $N$: $NCN^{-1}, NDN^{-1}, NEN^{-1}$.
- Use linear algebra to compute $NKN^{-1}$ (as we did for Scheme A).
- Compute $K$ from $NKN^{-1}$.

# Scheme B cryptanalysis

- Let's focus on Alice's subgroup $\mathcal{A} = M^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} M$.

# Scheme B cryptanalysis

- Let's focus on Alice's subgroup $\mathcal{A} = M^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} M$.
- Eve needs to find a matrix $N$ such that $\mathcal{A} = N^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} N$

# Scheme B cryptanalysis

- Let's focus on Alice's subgroup $\mathcal{A} = M^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} M$.
- Eve needs to find a matrix $N$ such that $\mathcal{A} = N^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} N$
- For some $U, V \in \mathrm{GL}_2(p)$, consider the matrix $N = \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix} M$.

# Scheme B cryptanalysis

- Let's focus on Alice's subgroup $\mathcal{A} = M^{-1} \left(\begin{smallmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{smallmatrix}\right) M$.
- Eve needs to find a matrix $N$ such that $\mathcal{A} = N^{-1} \left(\begin{smallmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{smallmatrix}\right) N$

- For some $U, V \in \mathrm{GL}_2(p)$, consider the matrix $N = \left(\begin{smallmatrix} U & 0 \\ 0 & V \end{smallmatrix}\right) M$.
- Then

$$N^{-1} \left(\begin{smallmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{smallmatrix}\right) N =$$

# Scheme B cryptanalysis

- Let's focus on Alice's subgroup $\mathcal{A} = M^{-1}\begin{pmatrix}\mathrm{SL}_2(p) & 0\\ 0 & I_2\end{pmatrix}M$.
- Eve needs to find a matrix $N$ such that $\mathcal{A} = N^{-1}\begin{pmatrix}\mathrm{SL}_2(p) & 0\\ 0 & I_2\end{pmatrix}N$
- For some $U, V \in \mathrm{GL}_2(p)$, consider the matrix $N = \begin{pmatrix}U & 0\\ 0 & V\end{pmatrix}M$.
- Then

$$N^{-1}\begin{pmatrix}\mathrm{SL}_2(p) & 0\\ 0 & I_2\end{pmatrix}N = M^{-1}\begin{pmatrix}U^{-1} & 0\\ 0 & V^{-1}\end{pmatrix}\begin{pmatrix}\mathrm{SL}_2(p) & 0\\ 0 & I_2\end{pmatrix}\begin{pmatrix}U & 0\\ 0 & V\end{pmatrix}M$$

# Scheme B cryptanalysis

- Let's focus on Alice's subgroup $\mathcal{A} = M^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} M$.
- Eve needs to find a matrix $N$ such that $\mathcal{A} = N^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} N$
- For some $U, V \in \mathrm{GL}_2(p)$, consider the matrix $N = \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix} M$.
- Then

$$\begin{aligned} N^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} N &= M^{-1} \begin{pmatrix} U^{-1} & 0 \\ 0 & V^{-1} \end{pmatrix} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix} M \\ &= M^{-1} \begin{pmatrix} U^{-1}\mathrm{SL}_2(p)U & 0 \\ 0 & V^{-1}V \end{pmatrix} M \end{aligned}$$

# Scheme B cryptanalysis

- Let's focus on Alice's subgroup $\mathcal{A} = M^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} M$.
- Eve needs to find a matrix $N$ such that $\mathcal{A} = N^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} N$
- For some $U, V \in \mathrm{GL}_2(p)$, consider the matrix $N = \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix} M$.
- Then

$$\begin{aligned} N^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} N &= M^{-1} \begin{pmatrix} U^{-1} & 0 \\ 0 & V^{-1} \end{pmatrix} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix} M \\ &= M^{-1} \begin{pmatrix} U^{-1}\mathrm{SL}_2(p)U & 0 \\ 0 & V^{-1}V \end{pmatrix} M \\ &= M^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} M \end{aligned}$$

# Scheme B cryptanalysis

- Let's focus on Alice's subgroup $\mathcal{A} = M^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} M$.
- Eve needs to find a matrix $N$ such that $\mathcal{A} = N^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} N$

- For some $U, V \in \mathrm{GL}_2(p)$, consider the matrix $N = \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix} M$.
- Then

$$\begin{aligned} N^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} N &= M^{-1} \begin{pmatrix} U^{-1} & 0 \\ 0 & V^{-1} \end{pmatrix} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix} M \\ &= M^{-1} \begin{pmatrix} U^{-1}\mathrm{SL}_2(p)U & 0 \\ 0 & V^{-1}V \end{pmatrix} M \\ &= M^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} M \\ &= \mathcal{A}. \end{aligned}$$

# Scheme B cryptanalysis

- Let's focus on Alice's subgroup $\mathcal{A} = M^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} M$.
- Eve needs to find a matrix $N$ such that $\mathcal{A} = N^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} N$

- For some $U, V \in \mathrm{GL}_2(p)$, consider the matrix $N = \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix} M$.
- Then

$$
\begin{aligned}
N^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} N &= M^{-1} \begin{pmatrix} U^{-1} & 0 \\ 0 & V^{-1} \end{pmatrix} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix} M \\
&= M^{-1} \begin{pmatrix} U^{-1}\mathrm{SL}_2(p)U & 0 \\ 0 & V^{-1}V \end{pmatrix} M \\
&= M^{-1} \begin{pmatrix} \mathrm{SL}_2(p) & 0 \\ 0 & I_2 \end{pmatrix} M \\
&= \mathcal{A}.
\end{aligned}
$$

- The same argument holds for $\mathcal{B}$.

# Scheme B cryptanalysis

- It suffices for Eve to find a matrix of the form $N = \left(\begin{smallmatrix} U & 0 \\ 0 & V \end{smallmatrix}\right) M$, for some $U, V \in \mathrm{GL}_2(p)$.

# Scheme B cryptanalysis

- It suffices for Eve to find a matrix of the form $N = \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix} M$, for some $U, V \in \mathrm{GL}_2(p)$.

- Let $M = \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix}$. Assume* $M_{11}$ and $M_{22}$ are invertible.

# Scheme B cryptanalysis

- It suffices for Eve to find a matrix of the form $N = \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix} M$, for some $U, V \in \mathrm{GL}_2(p)$.

- Let $M = \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix}$. Assume* $M_{11}$ and $M_{22}$ are invertible.

- Set $U = M_{11}^{-1}, V = M_{22}^{-1}$.

# Scheme B cryptanalysis

- It suffices for Eve to find a matrix of the form $N = \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix} M$, for some $U, V \in \mathrm{GL}_2(p)$.
- Let $M = \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix}$. Assume* $M_{11}$ and $M_{22}$ are invertible.
- Set $U = M_{11}^{-1}, V = M_{22}^{-1}$.
- So

$$\begin{aligned} N &= \begin{pmatrix} M_{11}^{-1} & 0 \\ 0 & M_{22}^{-1} \end{pmatrix} \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix} \\ &= \begin{pmatrix} I_2 & M_{11}^{-1} M_{12} \\ M_{22}^{-1} M_{21} & I_2 \end{pmatrix} \end{aligned}$$

# Scheme B cryptanalysis

- It suffices for Eve to find a matrix of the form $N = \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix} M$, for some $U, V \in \mathrm{GL}_2(p)$.

- Let $M = \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix}$. Assume* $M_{11}$ and $M_{22}$ are invertible.

- Set $U = M_{11}^{-1}, V = M_{22}^{-1}$.
- So

$$\begin{aligned} N &= \begin{pmatrix} M_{11}^{-1} & 0 \\ 0 & M_{22}^{-1} \end{pmatrix} \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix} \\ &= \begin{pmatrix} I_2 & M_{11}^{-1} M_{12} \\ M_{22}^{-1} M_{21} & I_2 \end{pmatrix} \\ &= \begin{pmatrix} I_2 & N_{12} \\ N_{21} & I_2 \end{pmatrix}. \end{aligned}$$

# Scheme B cryptanalysis

- So now Eve is looking for a matrix $N = \begin{pmatrix} I_2 & N_{12} \\ N_{21} & I_2 \end{pmatrix}$.

# Scheme B cryptanalysis

- So now Eve is looking for a matrix $N = \begin{pmatrix} I_2 & N_{12} \\ N_{21} & I_2 \end{pmatrix}$.

- Clearly Eve does not know $N^{-1}$. So we have 8 unknowns for $N$ and 16 unknowns for $N^{-1}$: a total of 24 unknowns.

# Scheme B cryptanalysis

- So now Eve is looking for a matrix $N = \begin{pmatrix} I_2 & N_{12} \\ N_{21} & I_2 \end{pmatrix}$.
- Clearly Eve does not know $N^{-1}$. So we have 8 unknowns for $N$ and 16 unknowns for $N^{-1}$: a total of 24 unknowns.
- From the transmitted matrices $C, D, E$, one can find 8 quadratic equations in the entries of $N$ and $N^{-1}$.

# Scheme B cryptanalysis

- So now Eve is looking for a matrix $N = \begin{pmatrix} I_2 & N_{12} \\ N_{21} & I_2 \end{pmatrix}$.
- Clearly Eve does not know $N^{-1}$. So we have 8 unknowns for $N$ and 16 unknowns for $N^{-1}$: a total of 24 unknowns.
- From the transmitted matrices $C, D, E$, one can find 8 quadratic equations in the entries of $N$ and $N^{-1}$.
- Furthermore, we require $N$ to be invertible, so we have 16 quadratic equations given by $NN^{-1} = I_4$.

# Scheme B cryptanalysis

- So now Eve is looking for a matrix $N = \begin{pmatrix} I_2 & N_{12} \\ N_{21} & I_2 \end{pmatrix}$.
- Clearly Eve does not know $N^{-1}$. So we have 8 unknowns for $N$ and 16 unknowns for $N^{-1}$: a total of 24 unknowns.
- From the transmitted matrices $C, D, E$, one can find 8 quadratic equations in the entries of $N$ and $N^{-1}$.
- Furthermore, we require $N$ to be invertible, so we have 16 quadratic equations given by $NN^{-1} = I_4$.
- This gives us 24 quadratic equations in 24 unknowns.

# Scheme B cryptanalysis

- We can solve this system of equations using Gröbner bases.
- Experimentally, over 1000 trials, each Gröbner basis calculation reveals a maximum of 6 possibilities for $N$ ($\approx$ 12 seconds for 300 bit prime $p$ on a standard PC in Magma).

# Scheme B cryptanalysis

- We can solve this system of equations using Gröbner bases.
- Experimentally, over 1000 trials, each Gröbner basis calculation reveals a maximum of 6 possibilities for $N$ ($\approx 12$ seconds for 300 bit prime $p$ on a standard PC in Magma).
- Observing another run of the protocol gives us 8 new equations. Adding these to the Gröbner basis calculation reveals a unique $N$.
- Scheme B is broken.

# So far so good..

- Recall: Scheme A $\subset$ Scheme B $\subset$ BCFRX Scheme, where:
- Scheme A is a public version of BCFRX over $\mathrm{SL}_4(p)$.
- Scheme B is a symmetric version of BCFRX over $\mathrm{SL}_4(p)$.
- Let's look at the BCFRX Scheme..

# BCFRX Scheme

- This is Scheme B but working over $\mathrm{SL}_4(\mathbb{Z})$ instead of $\mathrm{SL}_4(p)$. But $\mathrm{SL}_4(\mathbb{Z})$ is infinite!

# BCFRX Scheme

- This is Scheme B but working over $\mathrm{SL}_4(\mathbb{Z})$ instead of $\mathrm{SL}_4(p)$. But $\mathrm{SL}_4(\mathbb{Z})$ is infinite!

- However we sample $\mathrm{SL}_4(\mathbb{Z})$, in practice there is a bound $\Lambda$ on all matrices generated in the protocol. In particular $K = K \bmod \Lambda$.

# BCFRX Scheme

- This is Scheme B but working over $\mathrm{SL}_4(\mathbb{Z})$ instead of $\mathrm{SL}_4(p)$. But $\mathrm{SL}_4(\mathbb{Z})$ is infinite!
- However we sample $\mathrm{SL}_4(\mathbb{Z})$, in practice there is a bound $\Lambda$ on all matrices generated in the protocol. In particular $K = K \bmod \Lambda$.
- When presented with matrices $C, D, E$ from BCFRX Scheme, pick primes $p_i$ such that $\prod p_i > \Lambda$.

# BCFRX Scheme

- This is Scheme B but working over $\mathrm{SL}_4(\mathbb{Z})$ instead of $\mathrm{SL}_4(p)$. But $\mathrm{SL}_4(\mathbb{Z})$ is infinite!
- However we sample $\mathrm{SL}_4(\mathbb{Z})$, in practice there is a bound $\Lambda$ on all matrices generated in the protocol. In particular $K = K \bmod \Lambda$.
- When presented with matrices $C, D, E$ from BCFRX Scheme, pick primes $p_i$ such that $\prod p_i > \Lambda$.
- Compute $K$ mod $p_i$ as we did for Scheme B, followed by $K \bmod \prod p_i = K$ using Chinese Remainder Theorem.

# BCFRX Scheme

- This is Scheme B but working over $\mathrm{SL}_4(\mathbb{Z})$ instead of $\mathrm{SL}_4(p)$. But $\mathrm{SL}_4(\mathbb{Z})$ is infinite!
- However we sample $\mathrm{SL}_4(\mathbb{Z})$, in practice there is a bound $\Lambda$ on all matrices generated in the protocol. In particular $K = K \bmod \Lambda$.
- When presented with matrices $C, D, E$ from BCFRX Scheme, pick primes $p_i$ such that $\prod p_i > \Lambda$.
- Compute $K \bmod p_i$ as we did for Scheme B, followed by $K \bmod \prod p_i = K$ using Chinese Remainder Theorem.
- BCFRX Scheme is broken over $\mathrm{SL}_4(\mathbb{Z})$.

# HKS Scheme

- This is a public key agreement protocol.
- Quite abstact, involving semidirect products. But becomes transparent using suggested platform group $\mathrm{GL}_n(p)$.
- We describe (and cryptanalyse) the HKS Scheme based on $\mathrm{GL}_n(p)$ (and in a little more generality.)

# HKS Scheme

- We have public algorithms $M_A, M_B$ such that on all inputs, commuting matrices in $\mathrm{GL}_n(p)$ are output:

$$A \leftarrow M_A, \;\; B \leftarrow M_B, \;\; AB = BA.$$

# HKS Scheme

- We have public algorithms $M_A, M_B$ such that on all inputs, commuting matrices in $\mathrm{GL}_n(p)$ are output:

$$A \leftarrow M_A, \;\; B \leftarrow M_B, \;\; AB = BA.$$

- Let $b \in \mathbb{F}_p^n$ be public.
- Alice runs $M_A$ and sends $Ab$ to Bob.
- Bob runs $M_B$ and sends $Bb$ to Alice.

# HKS Scheme

- We have public algorithms $M_A, M_B$ such that on all inputs, commuting matrices in $\mathrm{GL}_n(p)$ are output:

$$A \leftarrow M_A, \;\; B \leftarrow M_B, \;\; AB = BA.$$

- Let $b \in \mathbb{F}_p^n$ be public.
- Alice runs $M_A$ and sends $Ab$ to Bob.
- Bob runs $M_B$ and sends $Bb$ to Alice.
- Alice computes $u = A(Bb)$. Bob computes $v = B(Ab)$.
- Since $A$ and $B$ commute, $u = v$ is their shared key.

# A cryptanalysis

Goal of passive adversary: given $b$, $u = Ab$, $v = Bb$, compute $k = ABb$.
Here's how:

# A cryptanalysis

Goal of passive adversary: given $b$, $u = Ab$, $v = Bb$, compute $k = ABb$.
Here's how:

- Eve samples $M_A$ to obtain matrices $A_1, A_2, \ldots$
  These matrices are guaranteed to commute with $B$.

# A cryptanalysis

Goal of passive adversary: given $b$, $u = Ab$, $v = Bb$, compute $k = ABb$. Here's how:

- Eve samples $M_A$ to obtain matrices $A_1, A_2, \ldots$
  These matrices are guaranteed to commute with $B$.

- Find $X$ such that:

$$XA_i = A_i X$$
$$Xb = v.$$

# A cryptanalysis

Goal of passive adversary: given $b$, $u = Ab$, $v = Bb$, compute $k = ABb$. Here's how:

- Eve samples $M_A$ to obtain matrices $A_1, A_2, \ldots$
  These matrices are guaranteed to commute with $B$.

- Find $X$ such that:

$$XA_i = A_i X$$
$$Xb = v.$$

- Note that a solution exists: $X = B$.
  Note that $X$ is <u>extremely</u> likely to commute with $A$.

# A cryptanalysis

Goal of passive adversary: given $b$, $u = Ab$, $v = Bb$, compute $k = ABb$. Here's how:

- Eve samples $M_A$ to obtain matrices $A_1, A_2, \ldots$
  These matrices are guaranteed to commute with $B$.

- Find $X$ such that:

$$XA_i = A_i X$$
$$Xb = v.$$

- Note that a solution exists: $X = B$.
  Note that $X$ is extremely likely to commute with $A$.
- Compute

$$Xu = XAb = AXb = Av = ABb = k.$$

# Summary

- We've seen two insecure matrix-based key establishment protocols.
- There are more! For example, Stickel's scheme (2004), Romanczuk–Ustimenko scheme (2010), Baba–Kotyad–Teja scheme (eprints 2011).

# Summary

- We've seen two insecure matrix-based key establishment protocols.
- There are more! For example, Stickel's scheme (2004), Romanczuk–Ustimenko scheme (2010), Baba–Kotyad–Teja scheme (eprints 2011).
- Conclusion: take care with matrices.

# Summary

- We've seen two insecure matrix-based key establishment protocols.
- There are more! For example, Stickel's scheme (2004), Romanczuk–Ustimenko scheme (2010), Baba–Kotyad–Teja scheme (eprints 2011).
- Conclusion: take care with matrices.

*-thanks for streaming!*