NTT

Quantum Algorithms for Fast Correlation Attacks on LFSR-Based Stream Ciphers

Akinori Hosoyamada

NTT Secure Platform Laboratories

December 11th, 2024 @ Asiacrypt 2024

Summary

- Quantum algorithms on fast correlation attacks by relating classical FFT (FWHT) with QFT (Hadamard operator)
- In Q1, it seems hard to achieve meaningful speed-up
- In Q2, introducing a special attack model, an interesting speed-up is obtained by using Shor's alg. for discrete log
- Complexity in Q2 is $O(\ell^4/c^2)$ for ℓ-bit LFSR, if a linear approximation of correlation c is available
- First quantum attack on SNOW 2.0 faster than Grover and current best (quantum) fast correlation attack on SNOW 3G

Quantum Backgrounds and Motivation of Research

Quantum Attack Models for Symmetric Cryptosystems

■ Q1

- Computers : Quantum
- Keyed oracles (enc, dec, prf, mac···) : Classical

■ Q2

- Both computers and keyed oracles are quantum: Quantum superposition queries are allowed
- Devastating polynomial-time attacks are possible (Even-Mansour, 4-round Luby-Rackoff, etc, are completely broken)
- Some important Q1 attacks are based on Q2 attacks

Quantum Attack Models for Symmetric Cryptosystems

NTT

- **Q1**
  - Computers : Quantum
  - Keyed oracles (enc, dec, prf, mac···) : Classical

- **Q2**
  - Both computers and keyed oracles are quantum: Quantum superposition queries are allowed
  - Devastating polynomial-time attacks are possible (Even-Mansour, 4-round Luby-Rackoff, etc, are completely broken)
  - Some important Q1 attacks are based on Q2 attacks

Studying Q2 attacks is important!

Recent Topics:
Classical Fourier Transform + QFT

Fourier Transform

Walsh-Hadamard Transform (WHT)

Strong relationship

Classical cryptanalytic techniques /notions

Linear correlations of block ciphers

Key-recovery of block ciphers

Recent Topics:
Classical Fourier Transform + QFT

Fourier Transform

Walsh-Hadamard Transform (WHT)

Strong relationship

Classical cryptanalytic techniques /notions

Linear correlations of block ciphers

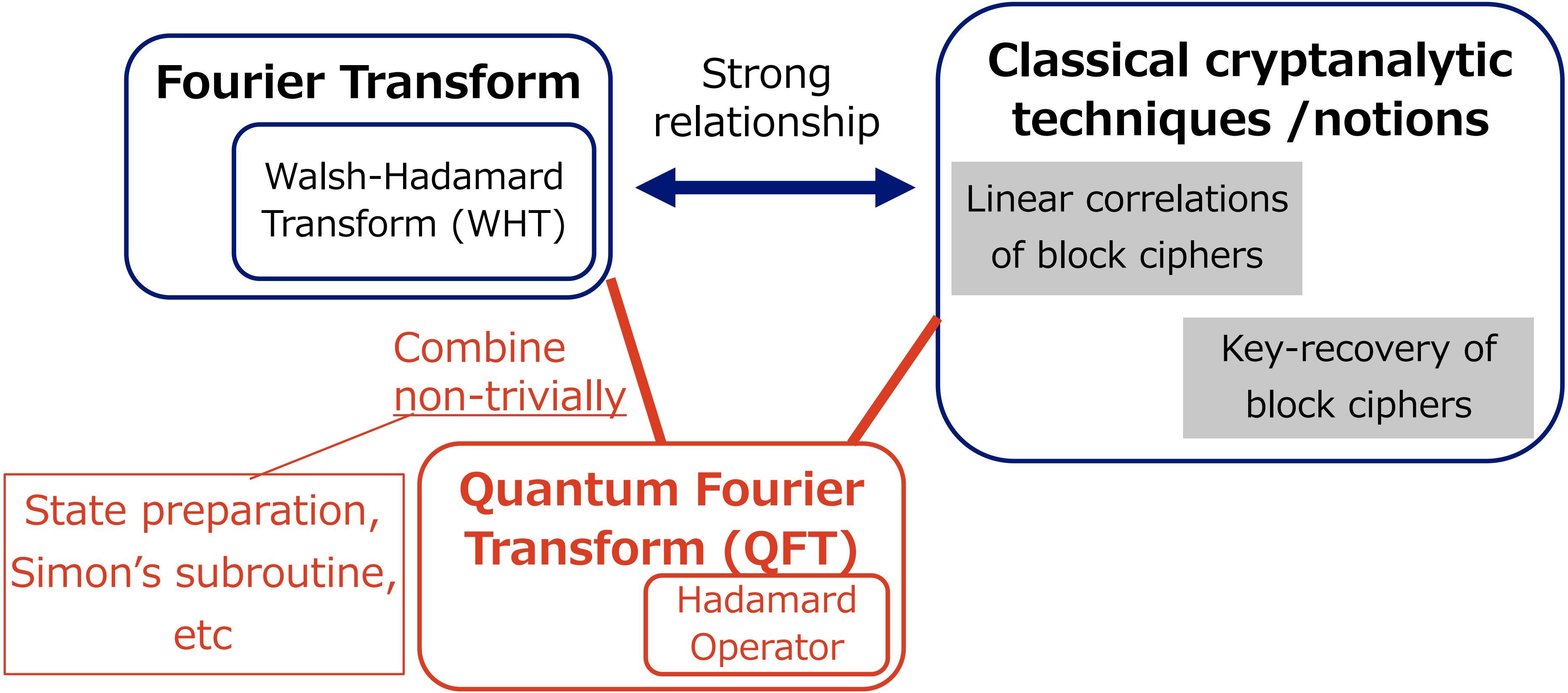
Key-recovery of block ciphers

Combine <u>non-trivially</u>

Quantum Fourier Transform (QFT)

Hadamard Operator

Recent Topics:
Classical Fourier Transform + QFT



Recent Topics:
Classical Fourier Transform + QFT

Fourier Transform

Walsh-Hadamard Transform (WHT)

Strong relationship

Classical cryptanalytic techniques /notions

Linear correlations of block ciphers

Key-recovery of block ciphers

Combine non-trivially

State preparation, Simon's subroutine, etc

Quantum Fourier Transform (QFT)

Hadamard Operator

Quantum speed-up for linear cryptanalysis [Sch23,Hos23]

Motivation of Research

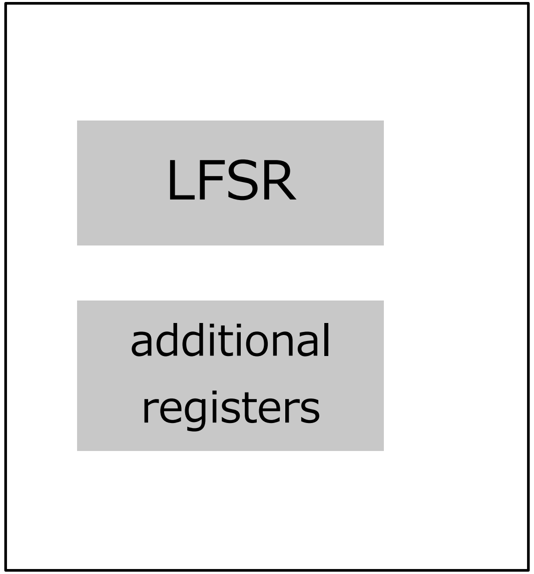
- Fast correlation attack [Sie84,MS88]: One of the most important attacks on LFSR-based stream ciphers
- Many fast correlation attacks also utilize FWHT

Question

Quantum speed-up for fast correlation attacks by combining classical Fourier transform (WHT) with QFT (Hadamard operator)?

LFSR-Based Stream Ciphers

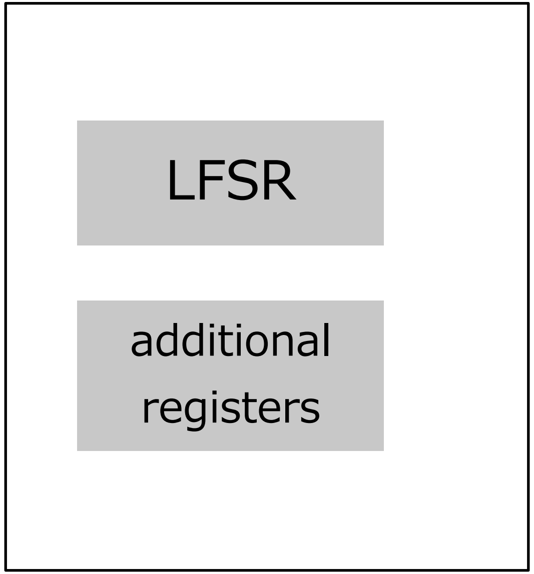
LFSR-Based Stream Cipher



LFSR-Based Stream Cipher

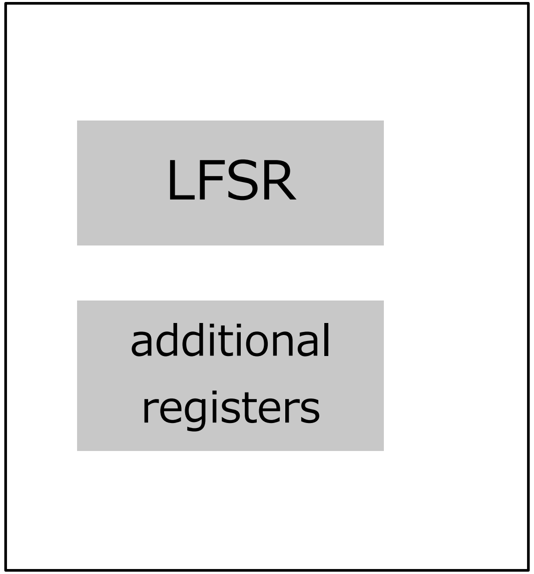
<u>Encryption procedure</u>

1. Initialization
2. Keystream generation
3. (Encryption)



LFSR-Based Stream Cipher

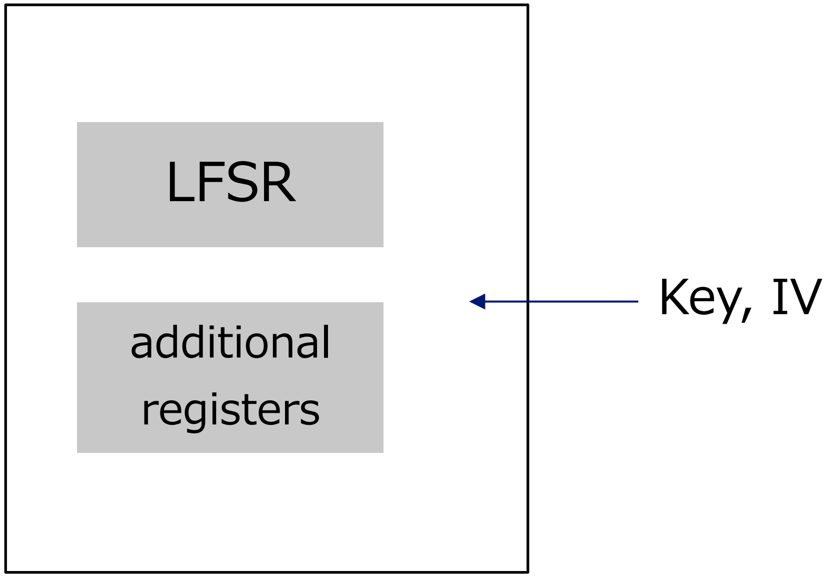
Initialization
1. Load master key & IV
2. Update state many times



LFSR-Based Stream Cipher

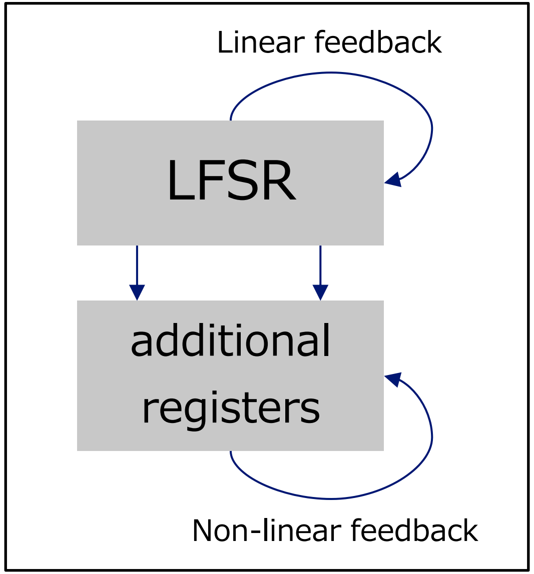
<u>Initialization</u>

1. Load master key & IV
2. Update state many times



LFSR-Based Stream Cipher

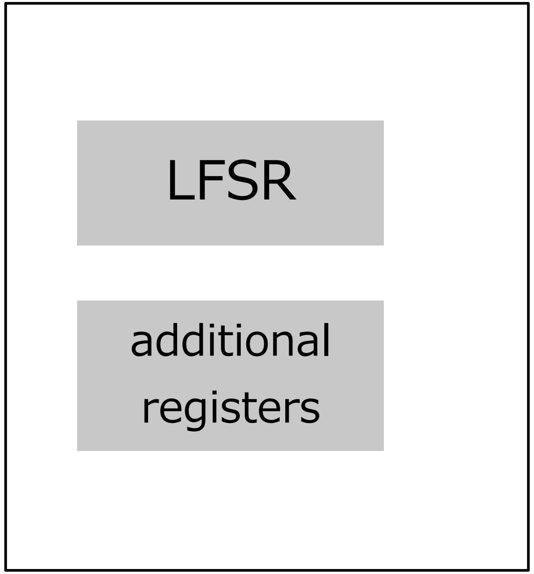
<u>Initialization</u>
1. Load master key & IV
2. Update state many times



LFSR-Based Stream Cipher

<u>Initialization</u>

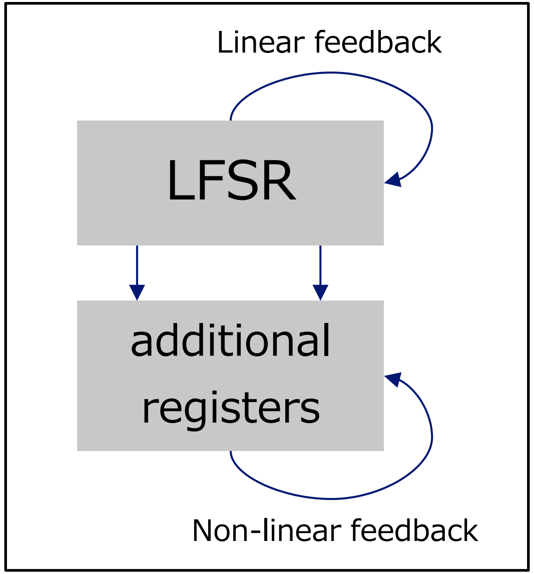
1. Load master key & IV
2. Update state many times



LFSR-Based Stream Cipher

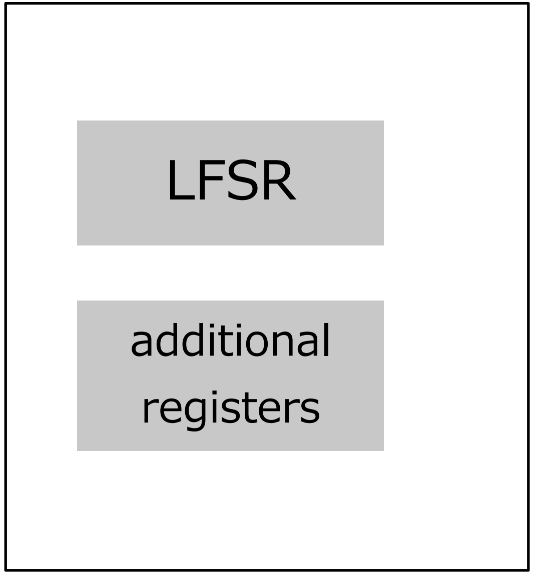
<u>Initialization</u>

1. Load master key & IV
2. Update state many times

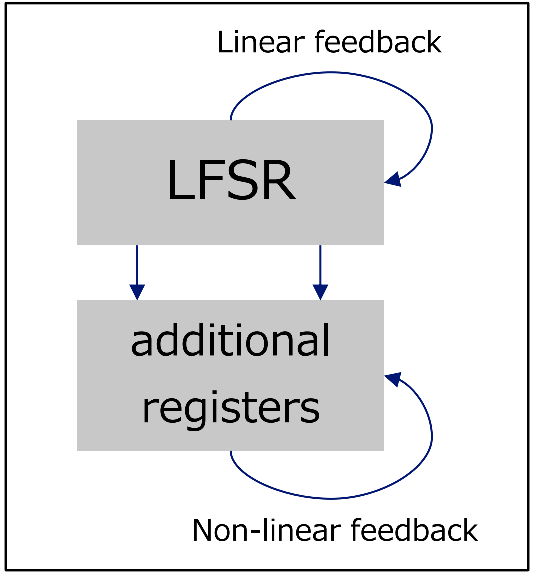


LFSR-Based Stream Cipher

Initialization
1. Load master key & IV
2. Update state many times



LFSR-Based Stream Cipher

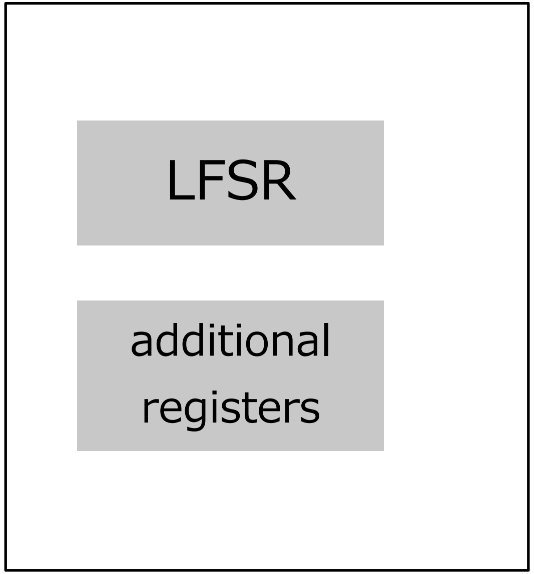


Initialization

1. Load master key & IV
2. Update state many times

LFSR-Based Stream Cipher

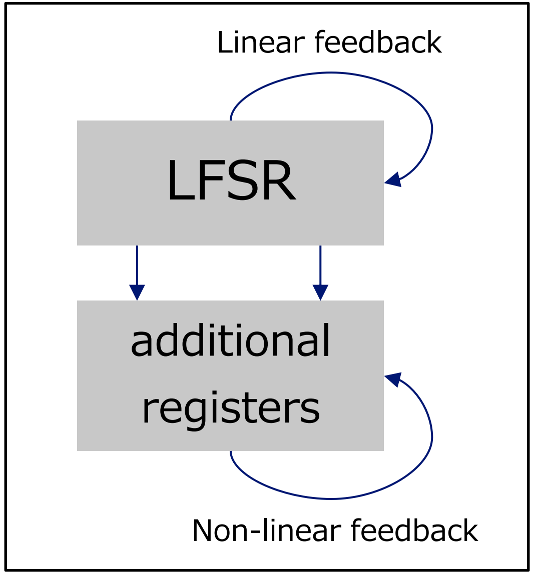
Initialization
1. Load master key & IV
2. Update state many times



LFSR-Based Stream Cipher

<u>Initialization</u>

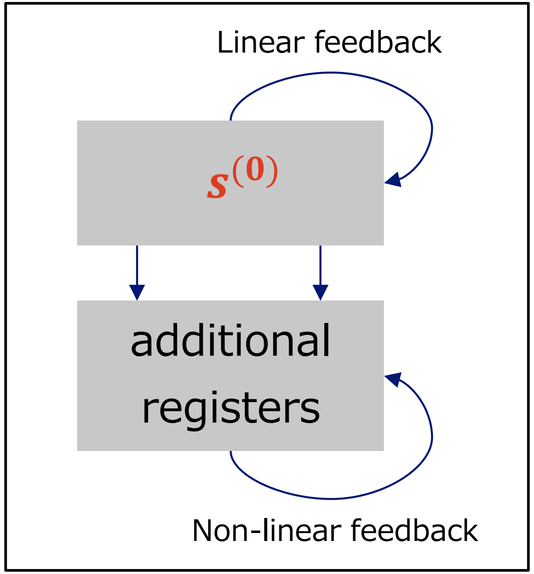
1. Load master key & IV
2. Update state many times



LFSR-Based Stream Cipher

<u>Initialization</u>

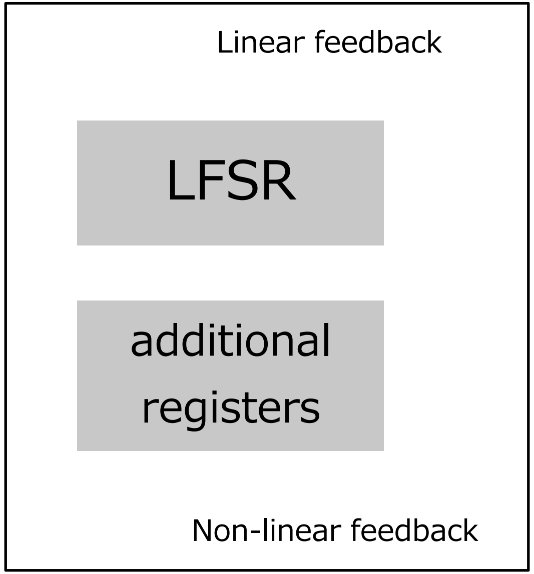
1. Load master key & IV
2. Update state many times



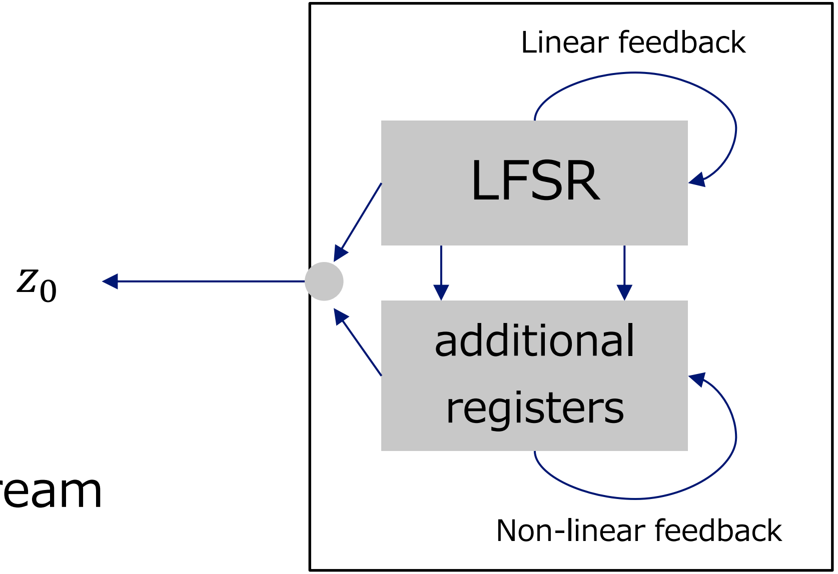
initial state

LFSR-Based Stream Cipher

Generate key stream



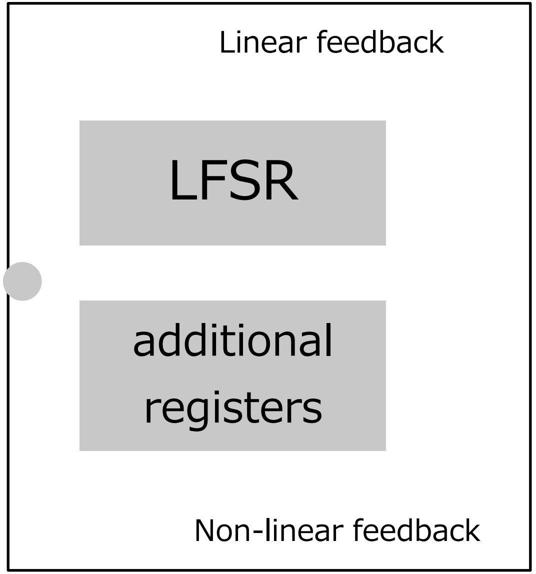
LFSR-Based Stream Cipher



Generate key stream

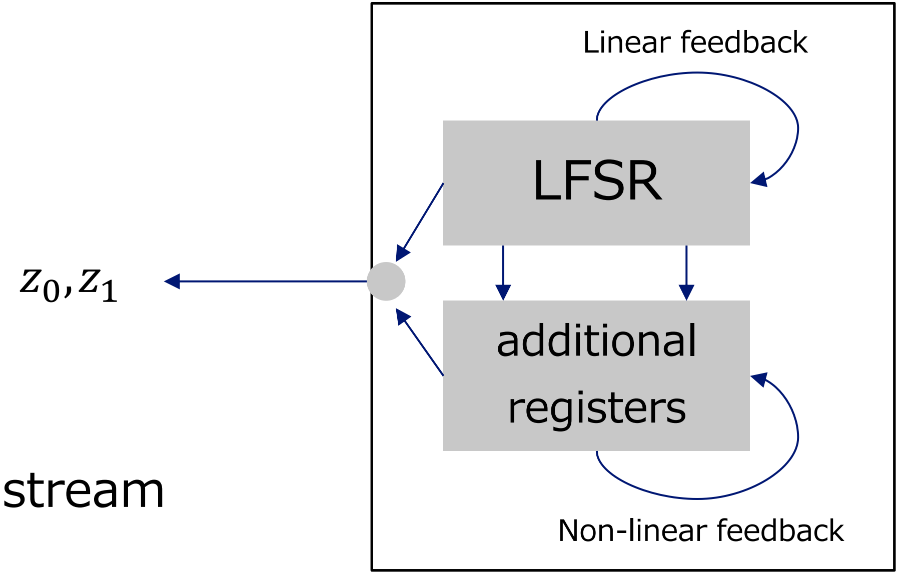
LFSR-Based Stream Cipher

z_0



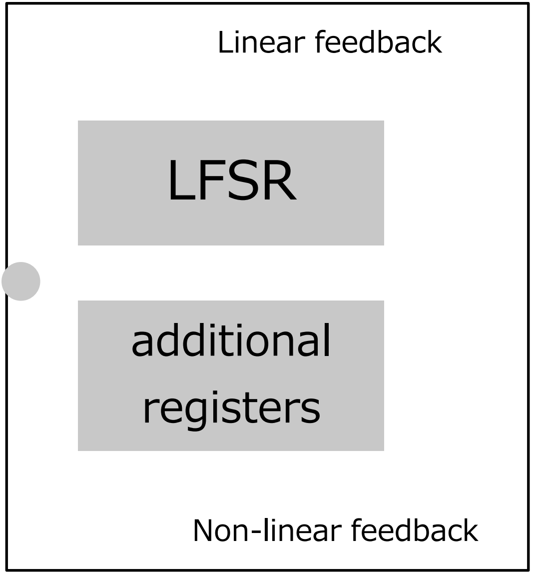
Generate key stream

LFSR-Based Stream Cipher



Generate key stream

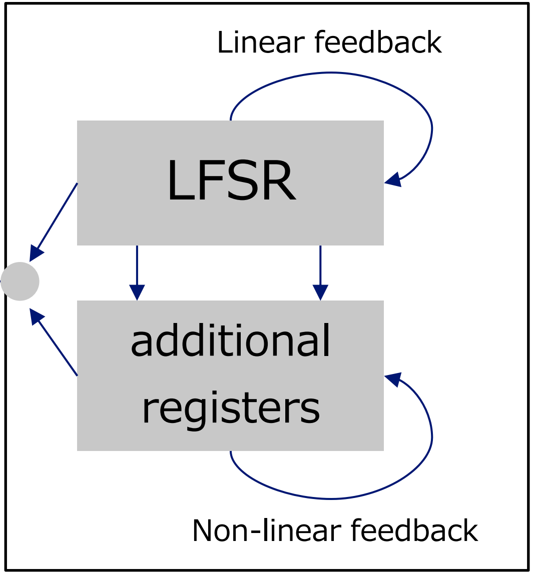
LFSR-Based Stream Cipher



z_0, z_1

Generate key stream

LFSR-Based Stream Cipher

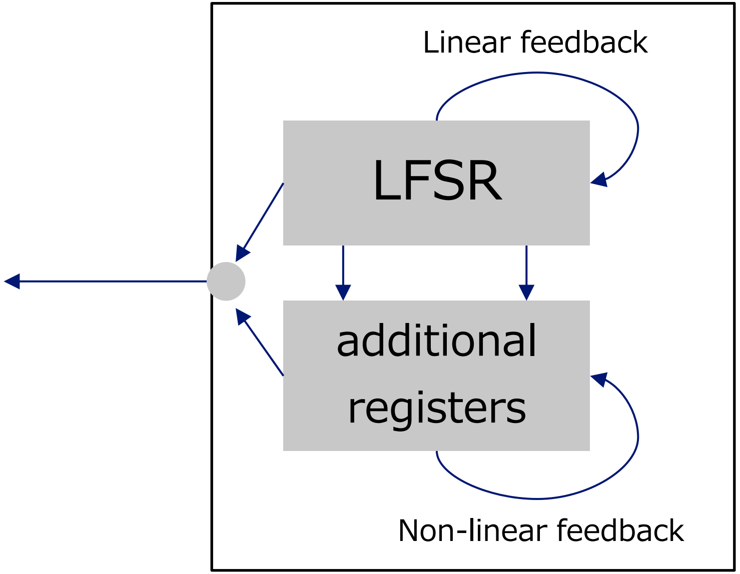


z_0, z_1, z_2

Generate key stream

LFSR-Based Stream Cipher

$z_0, z_1, \ldots, z_i, \ldots \ldots \ldots \ldots \ldots$

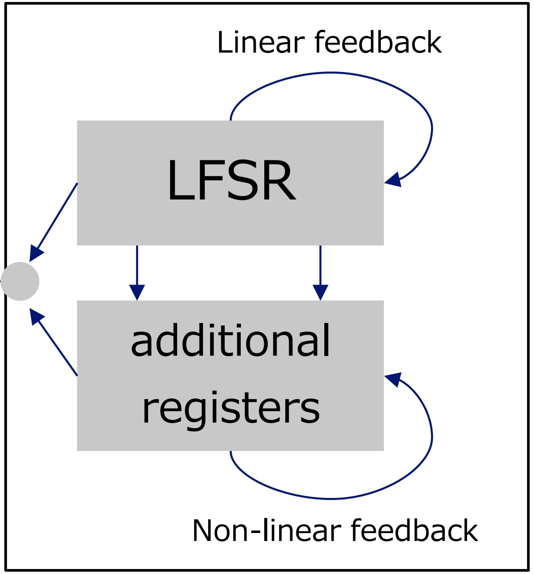


LFSR-Based Stream Cipher

Message M

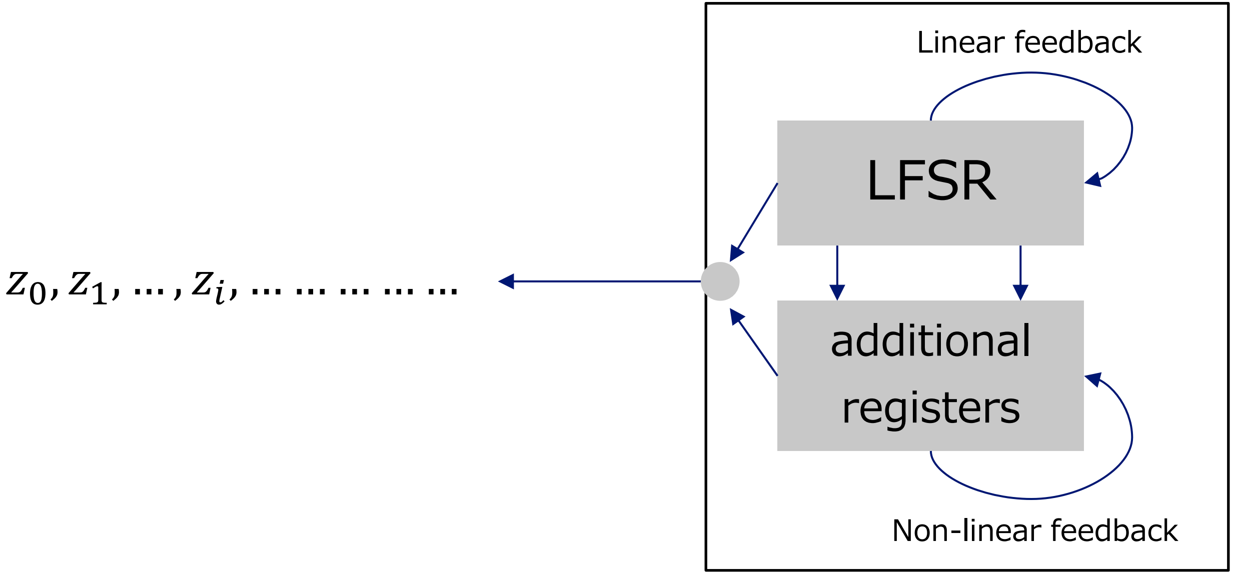
$z_0, z_1, \ldots, z_i, \ldots \ldots \ldots \ldots \ldots$

Ciphertext = M + keystream

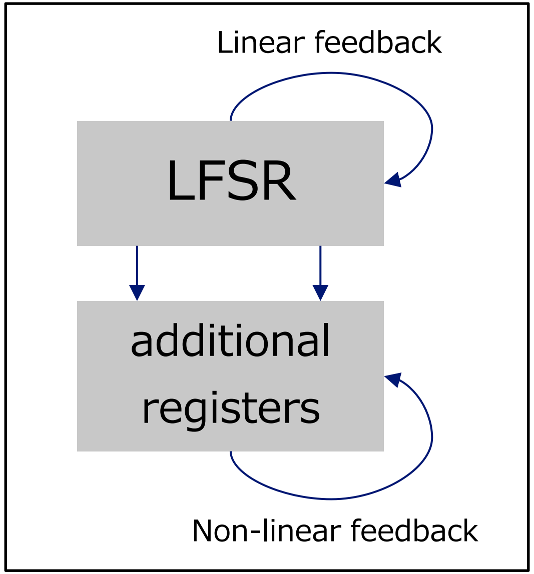


Fast Correlation Attack

LFSR-Based Stream Cipher

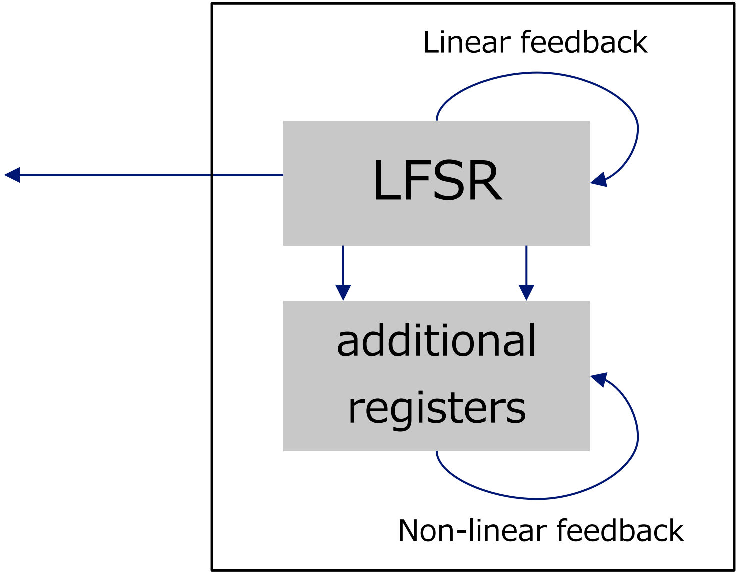


Alternative View

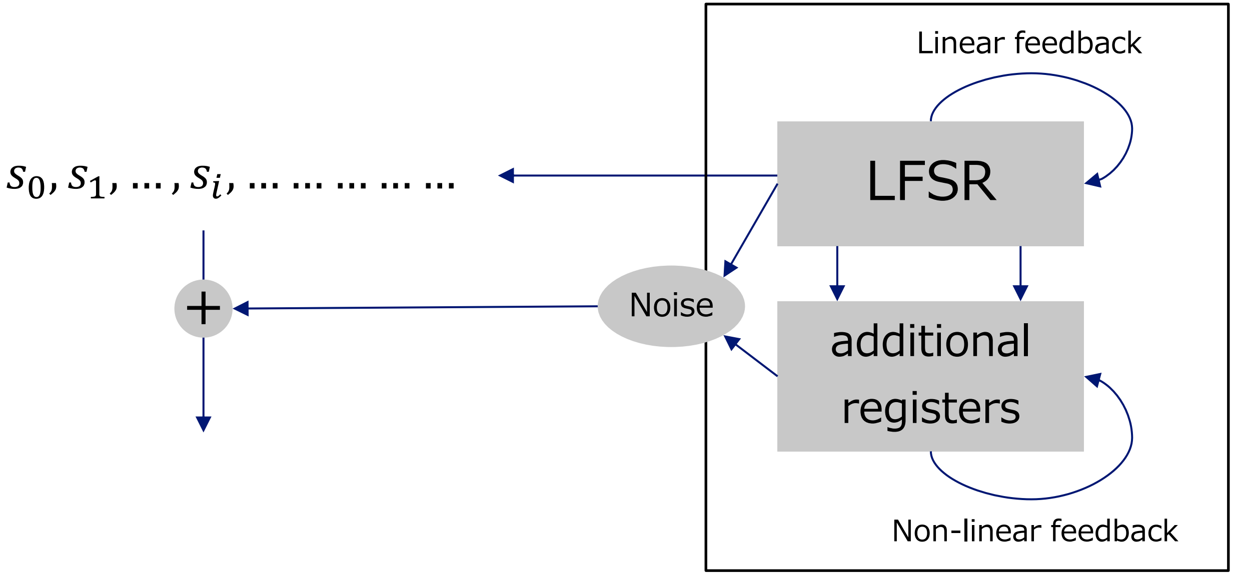


Alternative View

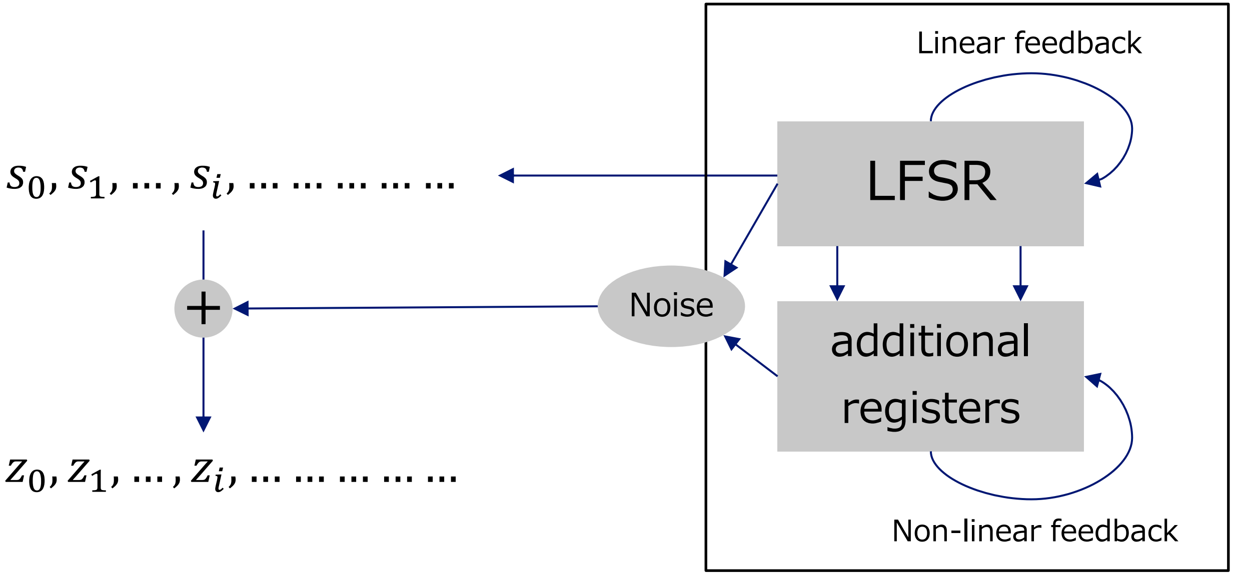
$s_0, s_1, \ldots, s_i, \ldots \ldots \ldots \ldots \ldots$



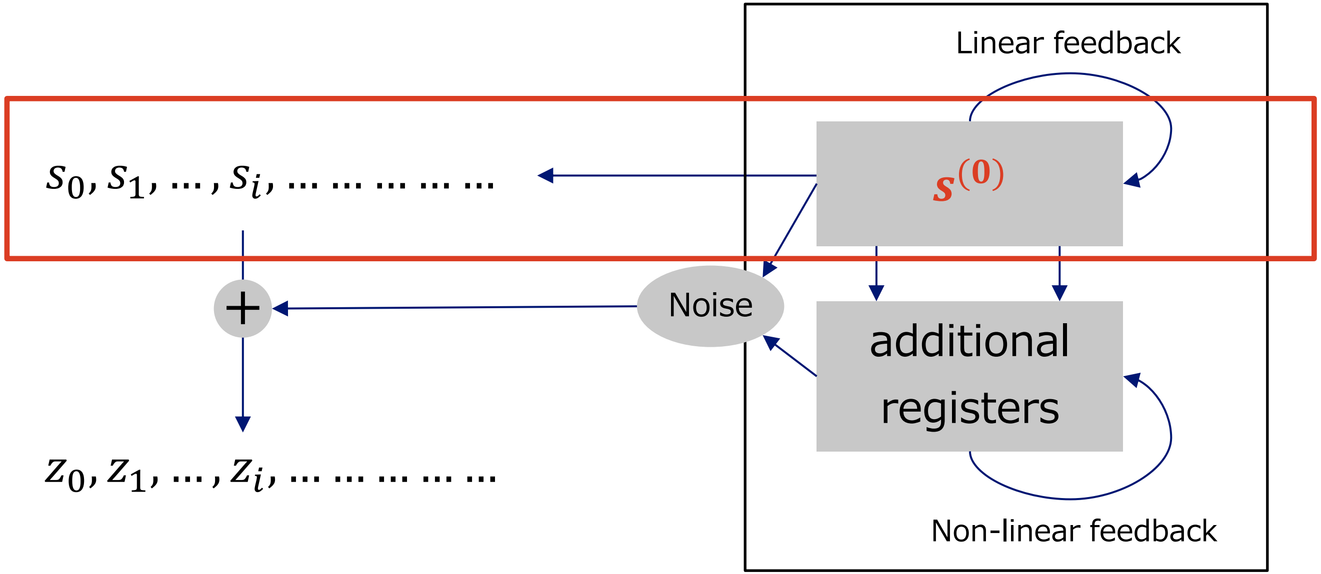
Alternative View



Alternative View

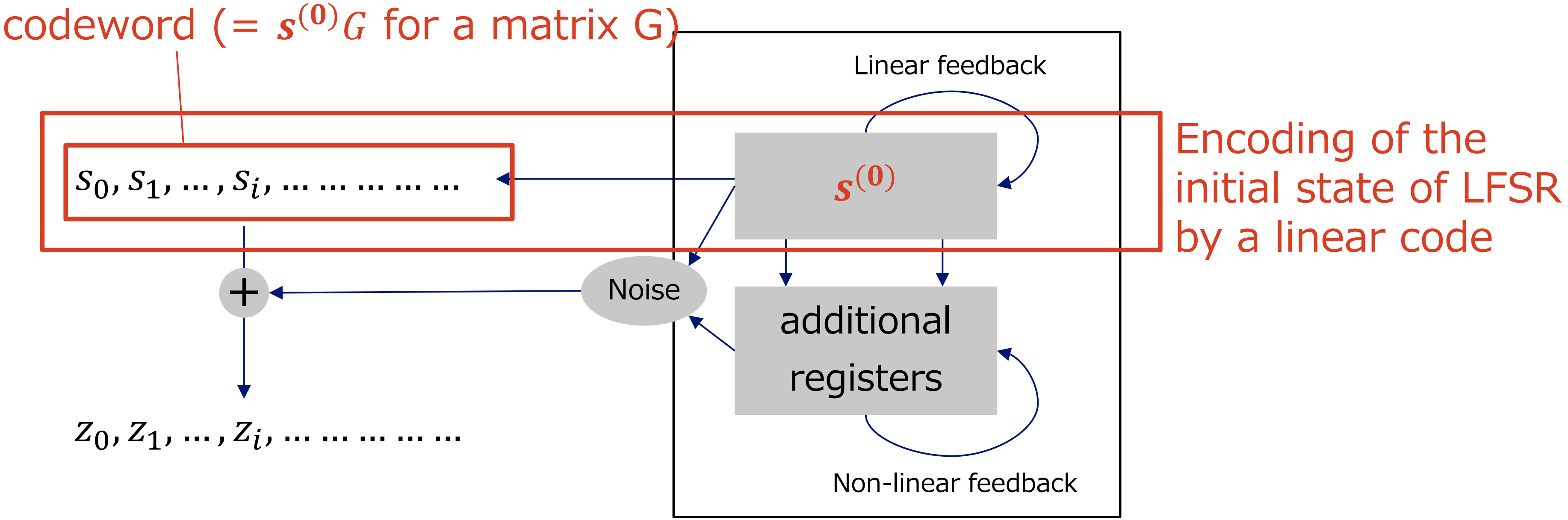


Alternative View

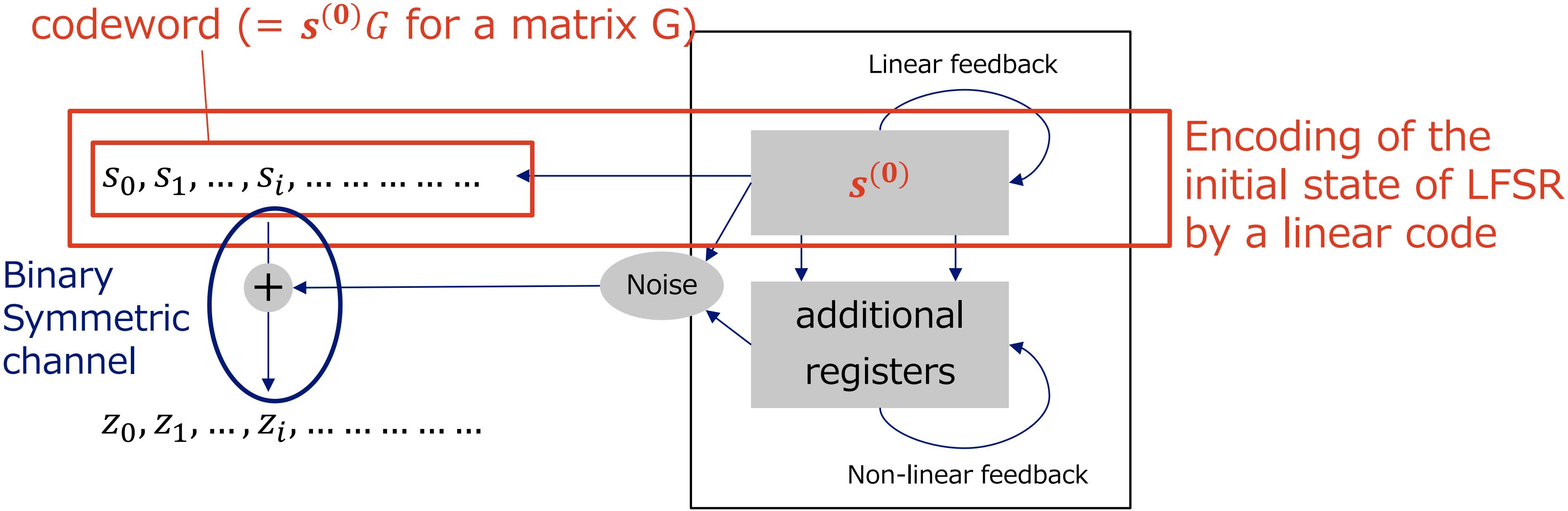


Encoding of the initial state of LFSR by a linear code

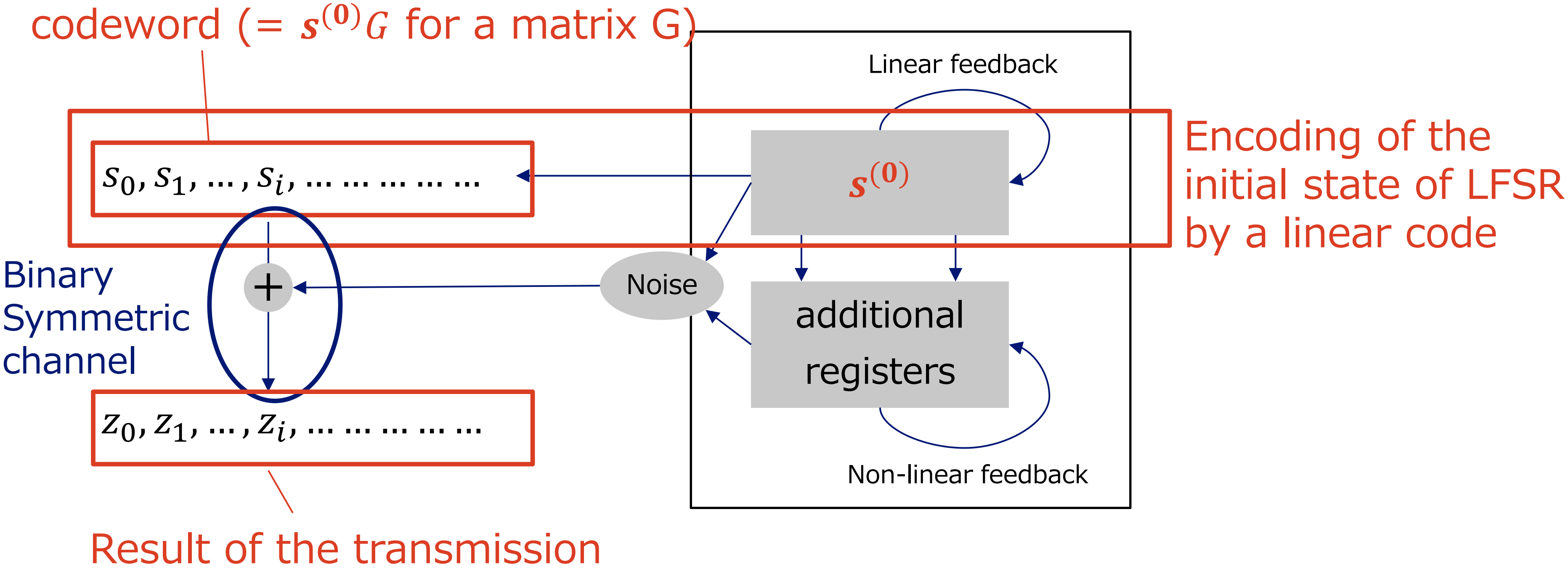
Alternative View



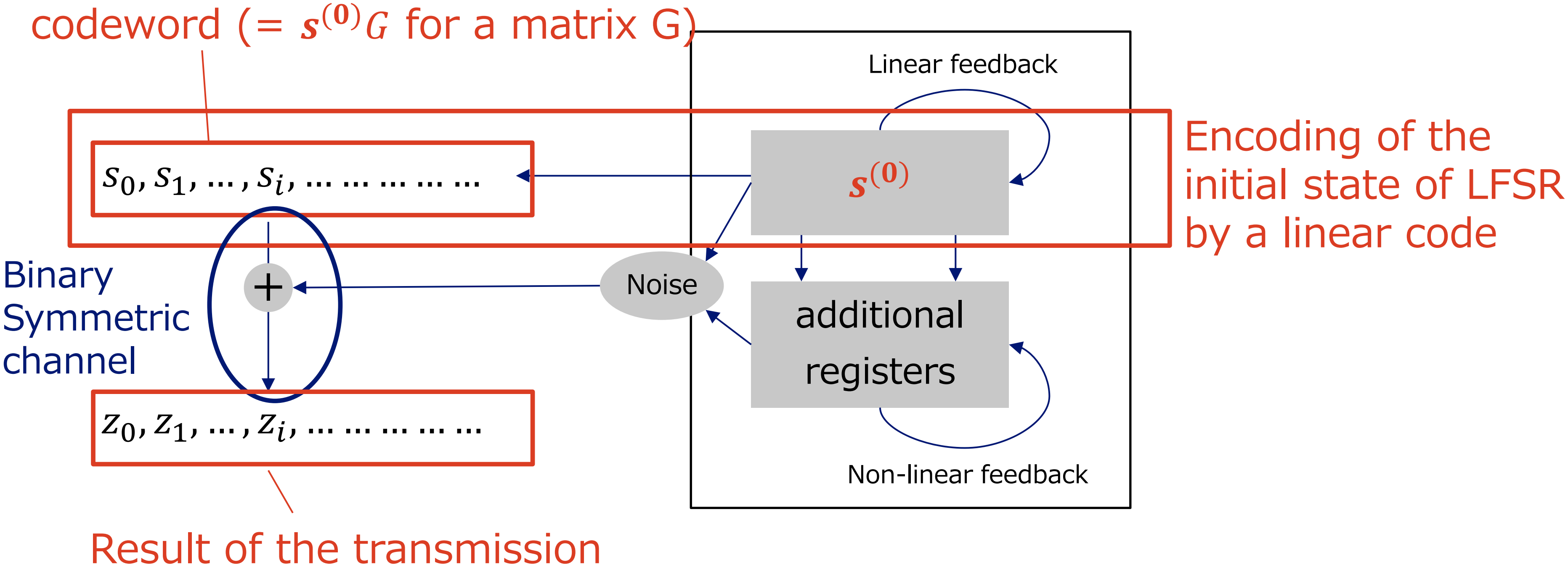
Alternative View



Alternative View



Alternative View



Idea:

If the noise is not too strong ($\Leftrightarrow$ the linear correlation $\mathrm{Cor}\left(\boldsymbol{s}^{(\mathbf{0})}G, \boldsymbol{z}\right)$ is large), the initial state of LFSR could be recovered by most-likelihood decoding

Decoding by FWHT to Recover $s^{(0)}$

NTT

- Assume ℓ -bit LFSR and we have $\boldsymbol{z} = (z_0, \ldots, z_{N-1})$ for some N
- G: the encoding matrix of the linear code (derived from LFSR), and $\boldsymbol{g}_i \in \mathbb{F}_2^\ell$: the i-th column of G

Define $\Psi: \mathbb{F}_2^\ell \to \mathbb{C}$ by

$$\Psi(\boldsymbol{w}) = \sum_{\substack{0 \le i \le N-1 \\ \boldsymbol{g}_i = \boldsymbol{w}}} (-1)^{z_i}$$

then we have

$$\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x}) \propto \mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})$$

Decoding by FWHT to Recover $s^{(0)}$

NTT

- Assume ℓ -bit LFSR and we have $\boldsymbol{z} = (z_0, \dots, z_{N-1})$ for some N
- G: the encoding matrix of the linear code (derived from LFSR), and $\boldsymbol{g}_i \in \mathbb{F}_2^\ell$: the i-th column of G

Define $\Psi\colon \mathbb{F}_2^\ell \to \mathbb{C}$ by

$$\Psi(\boldsymbol{w}) = \sum_{\substack{0 \le i \le N-1 \\ \boldsymbol{g}_i = \boldsymbol{w}}} (-1)^{z_i}$$

then we have

$$\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x}) \propto \underline{\mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})}$$

This value is large iff $\boldsymbol{x}$ equals the initial state of LFSR $\boldsymbol{s}^{(0)}$

Decoding by FWHT to Recover $s^{(0)}$

Decoding procedure:

1. Collect the key stream $\boldsymbol{z} = (z_0, \ldots, z_{N-1})$
2. Compute and store the value $\Psi(\boldsymbol{w})$ for all $\boldsymbol{w}$
3. Apply FWHT to Ψ, obtaining $\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x})$ for all $\boldsymbol{x}$
4. Output $\boldsymbol{x}$ with the largest $\left|\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x})\right|$ ($\rightarrow$ we get $\boldsymbol{s}^{(\mathbf{0})}$!)

Decoding by FWHT to Recover $s^{(0)}$

Decoding procedure:

1. Collect the key stream $\boldsymbol{z} = (z_0, \ldots, z_{N-1})$ N
2. Compute and store the value $\Psi(\boldsymbol{w})$ for all $\boldsymbol{w}$
3. Apply FWHT to Ψ, obtaining $\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x})$ for all $\boldsymbol{x}$
4. Output $\boldsymbol{x}$ with the largest $\left|\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x})\right|$ ($\rightarrow$ we get $\boldsymbol{s}^{(\mathbf{0})}$!)

Decoding by FWHT to Recover $s^{(0)}$

Decoding procedure:

1. Collect the key stream $\boldsymbol{z} = (z_0, \dots, z_{N-1})$ N
2. Compute and store the value $\Psi(\boldsymbol{w})$ for all $\boldsymbol{w}$ 2^ℓ
3. Apply FWHT to Ψ, obtaining $\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x})$ for all $\boldsymbol{x}$
4. Output $\boldsymbol{x}$ with the largest $\left|\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x})\right|$ ($\rightarrow$ we get $\boldsymbol{s}^{(0)}$!)

Decoding by FWHT to Recover $s^{(0)}$

Decoding procedure:

1. Collect the key stream $\boldsymbol{z} = (z_0, \dots, z_{N-1})$ N
2. Compute and store the value $\Psi(\boldsymbol{w})$ for all $\boldsymbol{w}$ 2^ℓ
3. Apply FWHT to Ψ, obtaining $\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x})$ for all $\boldsymbol{x}$ $\ell \cdot 2^\ell$
4. Output $\boldsymbol{x}$ with the largest $\big|\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x})\big|$ ($\rightarrow$ we get $\boldsymbol{s}^{(\mathbf{0})}$!)

Decoding by FWHT to Recover $s^{(0)}$

Decoding procedure:

1. Collect the key stream $\boldsymbol{z} = (z_0, \dots, z_{N-1})$ N
2. Compute and store the value $\Psi(\boldsymbol{w})$ for all $\boldsymbol{w}$ 2^ℓ
3. Apply FWHT to Ψ, obtaining $\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x})$ for all $\boldsymbol{x}$ $\ell \cdot 2^\ell$
4. Output $\boldsymbol{x}$ with the largest $\left|\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x})\right|$ ($\rightarrow$ we get $\boldsymbol{s}^{(0)}$!)
small

Decoding by FWHT to Recover $s^{(0)}$

NTT

Decoding procedure:

1. Collect the key stream $\boldsymbol{z} = (z_0, \dots, z_{N-1})$ N
2. Compute and store the value $\Psi(\boldsymbol{w})$ for all $\boldsymbol{w}$ 2^ℓ
3. Apply FWHT to Ψ, obtaining $\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x})$ for all $\boldsymbol{x}$ $\ell \cdot 2^\ell$
4. Output $\boldsymbol{x}$ with the largest $\left|\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x})\right|$ ($\rightarrow$ we get $\boldsymbol{s}^{(\mathbf{0})}$!) small

Complexity: $O(N + \ell 2^\ell)$

Decoding by FWHT to Recover $\boldsymbol{s}^{(\mathbf{0})}$

Decoding procedure:

1. Collect the key stream $\boldsymbol{z} = (z_0, \dots, z_{N-1})$ N
2. Compute and store the value $\Psi(\boldsymbol{w})$ for all $\boldsymbol{w}$ 2^ℓ
3. Apply FWHT to Ψ, obtaining $\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x})$ for all $\boldsymbol{x}$ $\ell \cdot 2^\ell$
4. Output $\boldsymbol{x}$ with the largest $\big|\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x})\big|$ ($\rightarrow$ we get $\boldsymbol{s}^{(\mathbf{0})}$!)

small

Complexity: $O(N + \ell 2^\ell)$

Succeeds with high probability if $N > \ell \cdot \mathrm{Cor}\big(\boldsymbol{s}^{(\mathbf{0})} G, \boldsymbol{z}\big)^{-2}$

Once the initial state of the LFSR $\boldsymbol{s}^{(\mathbf{0})}$ is recovered, the entire initial state is often easy to determine

Advanced Attack with Linear Approximation

- The attack works in the same way if there is a linear approximation between the LFSR output sequence and the keystream $\boldsymbol{z}$
- After a linear transform, $\boldsymbol{z}$ is again regarded as the encoding of $\boldsymbol{s}^{(\mathbf{0})}$ with some noise added
- The encoding matrix G=$(\boldsymbol{g}_1\ \boldsymbol{g}_2 \cdots \boldsymbol{g}_N)$ is given by

$$\boldsymbol{g_i} = \Gamma \cdot (M^\top)^{i-1} \quad (\in \mathbb{F}_2^L)$$

Γ : derived from linear mask

M :state update matrix of LFSR

Attempt of Quantum Speed-up in Q1

Classical Decoding to Recover $s^{(0)}$

NTT

Decoding procedure:

1. Collect the key stream $\boldsymbol{z} = (z_0, \ldots, z_{N-1})$ N
2. Compute and store the value $\Psi(\boldsymbol{w})$ for all $\boldsymbol{w}$ 2^ℓ
3. Apply FWHT to Ψ, obtaining $\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x})$ for all $\boldsymbol{x}$ $\ell \cdot 2^\ell$
4. Output $\boldsymbol{x}$ with the largest $\left|\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x})\right|$ ($\rightarrow$ we get $\boldsymbol{s}^{(0)}$!) small

Complexity: $O(N + \ell 2^\ell)$

Succeeds with high probability if $N > \ell \cdot \mathrm{Cor}\big(\boldsymbol{s}^{(0)}G, \boldsymbol{z}\big)^{-2}$

Classical Decoding to Recover $s^{(0)}$

Decoding procedure:

1. Collect the key stream $\boldsymbol{z} = (z_0, \dots, z_{N-1})$ N
2. Compute and store the value $\Psi(\boldsymbol{w})$ for all $\boldsymbol{w}$ 2^ℓ
3. Apply FWHT to Ψ, obtaining $\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x})$ for all $\boldsymbol{x}$ $\ell \cdot 2^\ell$
4. Output $\boldsymbol{x}$ with the largest $\left|\big(\mathrm{WHT}(\Psi)\big)(\boldsymbol{x})\right|$ ($\rightarrow$ we get $\boldsymbol{s}^{(0)}$!)

small

Complexity: $O(N + \ell 2^\ell)$

Succeeds with high probability if $N > \ell \cdot \mathrm{Cor}\big(\boldsymbol{s}^{(0)}G, \boldsymbol{z}\big)^{-2}$

We want a quantum speed-up
by replacing FWHT with Hadamard operator⋯

Attack Idea in Q1

1. Collect the key stream $\boldsymbol{z} = (z_0, \ldots, z_{N-1})$ and store it into qRAM (after applying some linear transform)
2. Prepare the state corresponding to the function Ψ, i.e.,
$$|\psi\rangle := \frac{1}{\sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{w}} \Psi(\boldsymbol{w}) |\boldsymbol{w}\rangle$$
3. Apply the Hadamard operator to obtain
$$H^{\otimes \ell} |\psi\rangle = \frac{N}{2^{\ell} \cdot \sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{x}} \mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z}) |\boldsymbol{x}\rangle$$
4. Amplify the amplitude of $\boldsymbol{x}$ with a large $\mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})$ (with QAA)

Attack Idea in Q1

(let $c := \mathrm{Cor}(\boldsymbol{s}^{(0)}G, \boldsymbol{z})$)

1. Collect the key stream $\boldsymbol{z} = (z_0, \ldots, z_{N-1})$ and store it into qRAM (after applying some linear transform)
2. Prepare the state corresponding to the function Ψ, i.e.,
$$|\psi\rangle := \frac{1}{\sqrt{\sum|\Psi(w)|^2}} \sum_{\boldsymbol{w}} \Psi(\boldsymbol{w})|\boldsymbol{w}\rangle$$
3. Apply the Hadamard operator to obtain
$$H^{\otimes \ell}|\psi\rangle = \frac{N}{2^{\ell} \cdot \sqrt{\sum|\Psi(w)|^2}} \sum_{\boldsymbol{x}} \mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})|\boldsymbol{x}\rangle$$
4. Amplify the amplitude of $\boldsymbol{x}$ with a large $\mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})$ (with QAA)

Attack Idea in Q1

(let $c := \mathrm{Cor}(\boldsymbol{s}^{(0)}G, \boldsymbol{z})$)

NTT

1. Collect the key stream $\boldsymbol{z} = (z_0, \ldots, z_{N-1})$ and store it into qRAM (after applying some linear transform) $N(> c^{-2})$
2. Prepare the state corresponding to the function Ψ, i.e.,

$$|\psi\rangle := \frac{1}{\sqrt{\sum|\Psi(w)|^2}} \sum_{\boldsymbol{w}} \Psi(\boldsymbol{w})|\boldsymbol{w}\rangle$$

3. Apply the Hadamard operator to obtain

$$H^{\otimes \ell}|\psi\rangle = \frac{N}{2^{\ell} \cdot \sqrt{\sum|\Psi(w)|^2}} \sum_{\boldsymbol{x}} \mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})|\boldsymbol{x}\rangle$$

4. Amplify the amplitude of $\boldsymbol{x}$ with a large $\mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})$ (with QAA)

Attack Idea in Q1

(let $c := \mathrm{Cor}(\boldsymbol{s}^{(0)}G, \boldsymbol{z})$)

NTT

1. Collect the key stream $\boldsymbol{z} = (z_0, \dots, z_{N-1})$ and store it into qRAM (after applying some linear transform) $N(> c^{-2})$
2. Prepare the state corresponding to the function Ψ, i.e.,

$$|\psi\rangle := \frac{1}{\sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{w}} \Psi(\boldsymbol{w}) |\boldsymbol{w}\rangle \qquad N$$

3. Apply the Hadamard operator to obtain

$$H^{\otimes \ell} |\psi\rangle = \frac{N}{2^{\ell} \cdot \sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{x}} \mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z}) |\boldsymbol{x}\rangle$$

4. Amplify the amplitude of $\boldsymbol{x}$ with a large $\mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})$ (with QAA)

Attack Idea in Q1

(let $c := \mathrm{Cor}(\boldsymbol{s}^{(0)}G, \boldsymbol{z})$)

NTT

1. Collect the key stream $\boldsymbol{z} = (z_0, \dots, z_{N-1})$ and store it into qRAM (after applying some linear transform) $N(> c^{-2})$
2. Prepare the state corresponding to the function Ψ, i.e.,
$$|\psi\rangle := \frac{1}{\sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{w}} \Psi(\boldsymbol{w}) |\boldsymbol{w}\rangle \quad N$$
3. Apply the Hadamard operator to obtain $\boldsymbol{O(1)}$
$$H^{\otimes \ell} |\psi\rangle = \frac{N}{2^{\ell} \cdot \sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{x}} \mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z}) |\boldsymbol{x}\rangle$$
4. Amplify the amplitude of $\boldsymbol{x}$ with a large $\mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})$ (with QAA)

Attack Idea in Q1

(let $c := \mathrm{Cor}(\boldsymbol{s}^{(0)}G, \boldsymbol{z})$)

NTT

1. Collect the key stream $\boldsymbol{z} = (z_0, \dots, z_{N-1})$ and store it into qRAM (after applying some linear transform) $N(> c^{-2})$
2. Prepare the state corresponding to the function Ψ, i.e.,
$$|\psi\rangle := \frac{1}{\sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{w}} \Psi(\boldsymbol{w}) |\boldsymbol{w}\rangle \quad N$$
3. Apply the Hadamard operator to obtain $\boldsymbol{O(1)}$
$$H^{\otimes \ell} |\psi\rangle = \frac{N}{2^{\ell} \cdot \sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{x}} \mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z}) |\boldsymbol{x}\rangle$$
4. Amplify the amplitude of $\boldsymbol{x}$ with a large $\mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})$ (with QAA)

$\gg 2^{\ell/2} / (N^{1/2} c)$

Attack Idea in Q1

(let $c \coloneqq \mathrm{Cor}(\boldsymbol{s}^{(0)}G, \boldsymbol{z})$)

NTT

1. Collect the key stream $\boldsymbol{z} = (z_0, \dots, z_{N-1})$ and store it into qRAM (after applying some linear transform) $N(> c^{-2})$
2. Prepare the state corresponding to the function Ψ, i.e.,

$$|\psi\rangle \coloneqq \frac{1}{\sqrt{\sum|\Psi(w)|^2}} \sum_{\boldsymbol{w}} \Psi(\boldsymbol{w})|\boldsymbol{w}\rangle \quad N$$

3. Apply the Hadamard operator to obtain $\boldsymbol{O(1)}$

$$H^{\otimes \ell}|\psi\rangle = \frac{N}{2^{\ell} \cdot \sqrt{\sum|\Psi(w)|^2}} \sum_{\boldsymbol{x}} \mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})|\boldsymbol{x}\rangle$$

4. Amplify the amplitude of $\boldsymbol{x}$ with a large $\mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})$ (with QAA)

$\gg 2^{\ell/2}/(N^{1/2}c)$

Overall complexity $\gg c^{-2} + (2^{\ell} \cdot c^{-2})^{1/3}$

$c^{-2} + \left(2^{\ell} \cdot c^{-2}\right)^{1/3}$ is Too Large...

- For some ciphers, c is so small that c^{-2} is larger than the complexity of the exhaustive key search with Grover's algorithm
- For others, ℓ is large (e.g., 512), so the term $\left(2^{\ell} \cdot c^{-2}\right)^{1/3}$ becomes too large
- It seems hard to obtain meaningful speed-up in Q1 (or, a completely different technique will be required)

$\rightarrow$ Let's move to Q2

New Attack Model in Q2

Search for Suitable Attack Model in Q2

- **【Classical】** The appropriate security notion for (IV-based) stream ciphers is the PRF security, regarding IVs as inputs and keystreams as outputs. [BG07]

$$IV \mapsto \boldsymbol{z}^{IV} = z_0^{IV} z_1^{IV} \cdots z_N^{IV}$$

Search for Suitable Attack Model in Q2

- **【Classical】** The appropriate security notion for (IV-based) stream ciphers is the PRF security, regarding IVs as inputs and keystreams as outputs. [BG07]

$$IV \mapsto \boldsymbol{z}^{IV} = z_0^{IV} z_1^{IV} \cdots z_N^{IV}$$

- **【Quantum/Q2】** Then, the corresponding attack model in Q2 would assume an oracle that receives quantum superposition of IVs and returns quantum superposition of keystreams⋯??

$$\sum_{IV} c_{IV} |IV\rangle \mapsto \sum_{IV} c_{IV} |IV\rangle \left|z_0^{IV} z_1^{IV} \cdots z_N^{IV}\right\rangle$$

Search for Suitable Attack Model in Q2

- 【**Quantum/Q2**】 Then, the corresponding attack model in Q2 would assume an oracle that receives quantum superposition of IVs and returns quantum superposition of keystreams···??

$$\sum_{IV} c_{IV} |IV\rangle \mapsto \sum_{IV} c_{IV} |IV\rangle \left| z_0^{IV} z_1^{IV} \cdots z_N^{IV} \right\rangle$$

- **Issues**: N operations needed solely for reading outputs, making the model essentially the same as Q1··· Moreover, the quantum computer is small while the register to receive z is very large, which is not reasonable

Search for Suitable Attack Model in Q2

Search for Suitable Attack Model in Q2

- 【**Alternative model**】Allow adversaries to query the index of the key stream

$$\sum_{\substack{IV \\ 0 \le i < 2^{\ell}}} c_{IV,i} |IV, \boldsymbol{i}\rangle \mapsto \sum_{\substack{IV \\ 0 \le i < 2^{\ell}}} c_{IV,i} |IV, i\rangle \left|z_i^{IV}\right\rangle$$

(remark: the parameter N now becomes 2^{ℓ})

- Feasibility: Some stream ciphers seem secure even in this model

Remark

- The purpose of studying attacks in this model is mainly to understand the power of Q2 attacks better, and make a basis of other attacks in future works
- We do not claim that the practical security of a cipher is affected even if it is broken in this model

Fast Correlation Attacks in Q2

Attack Idea in Q1

$c := \mathrm{Cor}(\boldsymbol{s}^{(0)}G, \boldsymbol{z})$

NTT

1. Collect the key stream $\boldsymbol{z} = (z_0, \ldots, z_{N-1})$ and store it into qRAM (after applying some linear transform) $N(> c^{-2})$
2. Prepare the state corresponding to the function Ψ, i.e.,
$$|\psi\rangle := \frac{1}{\sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{w}} \Psi(\boldsymbol{w}) |\boldsymbol{w}\rangle \quad N$$
3. Apply the Hadamard operator to obtain $O(1)$
$$H^{\otimes \ell} |\psi\rangle = \frac{N}{2^{\ell} \cdot \sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{x}} \mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z}) |\boldsymbol{x}\rangle$$
4. Amplify the amplitude of $\boldsymbol{x}$ with a large $\mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})$ (with QAA)

$\gg 2^{\ell/2} / (N^{1/2} c)$

Attack Idea in Q2

$c := \mathrm{Cor}(\boldsymbol{s}^{(0)}G, \boldsymbol{z})$

NTT

1. Collect the key stream $\boldsymbol{z} = (z_0, \ldots, z_{N-1})$ and store it into qRAM (after applying some linear transform) $N(> c^{-2})$
2. Prepare the state corresponding to the function Ψ, i.e.,
$$|\psi\rangle := \frac{1}{\sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{w}} \Psi(\boldsymbol{w}) |\boldsymbol{w}\rangle \qquad N$$
3. Apply the Hadamard operator to obtain $O(1)$
$$H^{\otimes \ell} |\psi\rangle = \frac{N}{2^{\ell} \cdot \sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{x}} \mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z}) |\boldsymbol{x}\rangle$$
4. Amplify the amplitude of $\boldsymbol{x}$ with a large $\mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})$ (with QAA)

$\gg 2^{\ell/2} / (N^{1/2} c)$

Attack Idea in Q2

$c := \mathrm{Cor}(\boldsymbol{s}^{(0)}G, \boldsymbol{z})$

~~1. Collect the key stream $z = ($~~
~~qRAM (after applying some~~

We can access all z_i simultaneously in quantum superposition

2. Prepare the state corresponding to the function Ψ, i.e.,

$$|\psi\rangle := \frac{1}{\sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{w}} \Psi(\boldsymbol{w}) |\boldsymbol{w}\rangle$$

3. Apply the Hadamard operator to obtain

$$H^{\otimes \ell} |\psi\rangle = \frac{N}{2^{\ell} \cdot \sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{x}} \mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z}) |\boldsymbol{x}\rangle$$

4. Amplify the amplitude of $\boldsymbol{x}$ with a large $\mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})$ (with QAA)

Attack Idea in Q2

$c := \mathrm{Cor}(\boldsymbol{s}^{(0)}G, \boldsymbol{z})$

~~1. Collect the key stream $z = ($~~
~~qRAM (after applying some~~

We can access all z_i simultaneously in quantum superposition

2. Prepare the state corresponding to the function Ψ, i.e.,

$$|\psi\rangle := \frac{1}{\sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{w}} \Psi(\boldsymbol{w}) |\boldsymbol{w}\rangle$$

3. Apply the Hadamard operator to obtain

$$H^{\otimes \ell} |\psi\rangle = \frac{N}{2^{\ell} \cdot \sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{x}} \overbrace{\mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})}^{O(1)} |\boldsymbol{x}\rangle$$

4. Amplify the amplitude of $\boldsymbol{x}$ with a large $\mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})$ (with QAA)

Attack Idea in Q2

$c := \mathrm{Cor}(\boldsymbol{s}^{(0)}G, \boldsymbol{z})$

NTT

1. ~~Collect the key stream $\boldsymbol{z} = (z$~~ ~~qRAM (after applying some~~

We can access all z_i simultaneously in quantum superposition

2. Prepare the state corresponding to the function Ψ, i.e.,

$$|\psi\rangle := \frac{1}{\sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{w}} \Psi(\boldsymbol{w}) |\boldsymbol{w}\rangle$$

3. Apply the Hadamard operator to obtain

$$H^{\otimes \ell} |\psi\rangle = \frac{N}{2^{\ell} \cdot \sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{x}} \mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z}) |\boldsymbol{x}\rangle$$

$O(1)$

4. Amplify the amplitude of $\boldsymbol{x}$ with a large $\mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})$ (with QAA)

$\mathrm{poly}(\ell) \cdot c^{-1}(c^{-1} + (\text{Step 2} + \text{Step 3}))$
by applying quantum counting

Attack Idea in Q2

$c := \mathrm{Cor}(\boldsymbol{s}^{(0)}G, \boldsymbol{z})$

~~1. Collect the key stream $z = ($~~
~~qRAM (after applying some~~

We can access all z_i simultaneously in quantum superposition

2. Prepare the state corresponding to the function Ψ, i.e.,

$$|\psi\rangle := \frac{1}{\sqrt{\sum|\Psi(w)|^2}} \sum_{\boldsymbol{w}} \Psi(\boldsymbol{w})|\boldsymbol{w}\rangle$$

$\mathrm{poly}(\ell)$

by applying Shor's algorithm

3. Apply the Hadamard operator to obtain

$O(1)$

$$H^{\otimes \ell}|\psi\rangle = \frac{N}{2^{\ell} \cdot \sqrt{\sum|\Psi(w)|^2}} \sum_{\boldsymbol{x}} \mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})|\boldsymbol{x}\rangle$$

4. Amplify the amplitude of $\boldsymbol{x}$ with a large $\mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})$ (with QAA)

$\mathrm{poly}(\ell) \cdot c^{-1}(c^{-1} + (\text{Step 2} + \text{Step 3}))$

by applying quantum counting

Preparation of $|\psi\rangle$ w/ Shor's Algorithm

$$\Psi(\boldsymbol{w}) = \sum_{\substack{0 \le i < 2^{\ell} \\ \boldsymbol{g}_i = \boldsymbol{w}}} (-1)^{z_i}$$

Preparation of $|\psi\rangle$ w/ Shor's Algorithm

NTT

$$\Psi(\boldsymbol{w}) = \sum_{\substack{0 \le i < 2^\ell \\ \boxed{\boldsymbol{g}_i = \boldsymbol{w}}}} (-1)^{z_i}$$

For each $\boldsymbol{w}$, we have to determine the index i s.t. $\boldsymbol{w}$ equals $\boldsymbol{g}_i$, the i-th column of the encoding matrix G

Preparation of $|\psi\rangle$ w/ Shor's Algorithm

$$\Psi(\boldsymbol{w}) = \sum_{\substack{0 \le i < 2^{\ell} \\ \boxed{\boldsymbol{g}_i = \boldsymbol{w}}}} (-1)^{z_i}$$

For each $\boldsymbol{w}$, we have to determine the index i s.t.
$\boldsymbol{w}$ equals $\boldsymbol{g}_i$, the i-th column of the encoding matrix G

$$\boldsymbol{g}_i = \Gamma \cdot (M^{\top})^{i-1} \quad \left(\in \mathbb{F}_2^{\ell}\right)$$

Preparation of $|\psi\rangle$ w/ Shor's Algorithm

$$\Psi(\boldsymbol{w}) = \sum_{\substack{0 \le i < 2^{\ell} \\ \boxed{\boldsymbol{g}_i = \boldsymbol{w}}}} (-1)^{z_i}$$

For each $\boldsymbol{w}$, we have to determine the index i s.t. $\boldsymbol{w}$ equals $\boldsymbol{g}_i$, the i-th column of the encoding matrix G

Γ : derived from linear mask

$$\boldsymbol{g_i} = \Gamma \cdot (M^{\top})^{i-1} \quad \left(\in \mathbb{F}_2^{\ell}\right)$$

Preparation of $|\psi\rangle$ w/ Shor's Algorithm

NTT

$$\Psi(\boldsymbol{w}) = \sum_{\substack{0 \le i < 2^{\ell} \\ \boxed{\boldsymbol{g}_i = \boldsymbol{w}}}} (-1)^{z_i}$$

For each $\boldsymbol{w}$, we have to determine the index i s.t.
$\boldsymbol{w}$ equals $\boldsymbol{g}_i$, the i-th column of the encoding matrix G

Γ : derived from linear mask

M :state update matrix of LFSR

$$\boldsymbol{g}_{\boldsymbol{i}} = \Gamma \cdot (M^{\top})^{i-1} \quad \left(\in \mathbb{F}_2^{\ell}\right)$$

Preparation of $|\psi\rangle$ w/ Shor's Algorithm

$$\Psi(\boldsymbol{w}) = \sum_{\substack{0 \le i < 2^\ell \\ \boxed{\boldsymbol{g}_i = \boldsymbol{w}}}} (-1)^{z_i}$$

For each $\boldsymbol{w}$, we have to determine the index i s.t. $\boldsymbol{w}$ equals $\boldsymbol{g}_i$, the i-th column of the encoding matrix G

Γ : derived from linear mask

M :state update matrix of LFSR

$$\boldsymbol{g}_i = \Gamma \cdot (M^\top)^{i-1} \quad \left(\in \mathbb{F}_2^\ell\right)$$

Multiplying $M^\top$ corresponds to multiplying the generator α of $\left(\mathbb{F}_{2^\ell}\right)^\times$

Preparation of $|\psi\rangle$ w/ Shor's Algorithm

$$\Psi(\boldsymbol{w}) = \sum_{\substack{0 \le i < 2^\ell \\ \boxed{\boldsymbol{g}_i = \boldsymbol{w}}}} (-1)^{z_i}$$

For each $\boldsymbol{w}$, we have to determine the index i s.t.
$\boldsymbol{w}$ equals $\boldsymbol{g}_i$, the i-th column of the encoding matrix G

Γ : derived from linear mask

M :state update matrix of LFSR

$$\boldsymbol{g_i} = \Gamma \cdot (M^\top)^{i-1} \quad \left(\in \mathbb{F}_2^\ell\right)$$
$$= \Gamma \cdot \alpha^{i-1} \quad \left(\in \mathbb{F}_{2^\ell}\right)$$

Multiplying $M^\top$ corresponds to multiplying the generator α of $\left(\mathbb{F}_{2^\ell}\right)^\times$

Preparation of $|\psi\rangle$ w/ Shor's Algorithm

$$\Psi(\boldsymbol{w}) = \sum_{\substack{0 \le i < 2^{\ell} \\ \boxed{\boldsymbol{g}_i = \boldsymbol{w}}}} (-1)^{z_i}$$

For each $\boldsymbol{w}$, we have to determine the index i s.t.
$\boldsymbol{w}$ equals $\boldsymbol{g}_i$, the i-th column of the encoding matrix G

Γ : derived from linear mask

M :state update matrix of LFSR

$$\boldsymbol{g}_i = \Gamma \cdot (M^{\top})^{i-1} \quad (\in \mathbb{F}_2^{\ell})$$
$$= \Gamma \cdot \alpha^{i-1} \quad (\in \mathbb{F}_{2^{\ell}})$$

$$i = \log_{\alpha}(\boldsymbol{g}_i) - \log_{\alpha}(\Gamma) + 1$$

Multiplying $M^{\top}$ corresponds to multiplying the generator α of $(\mathbb{F}_{2^{\ell}})^{\times}$

Preparation of $|\psi\rangle$ w/ Shor's Algorithm

NTT

$$\Psi(\boldsymbol{w}) = \sum_{\substack{0\le i<2^\ell \\ \boxed{\boldsymbol{g}_i=\boldsymbol{w}}}} (-1)^{z_i}$$

For each $\boldsymbol{w}$, we have to determine the index i s.t. $\boldsymbol{w}$ equals $\boldsymbol{g}_i$, the i-th column of the encoding matrix G

Γ : derived from linear mask

M :state update matrix of LFSR

$$\boldsymbol{g_i} = \Gamma \cdot (M^\top)^{i-1} \quad (\in \mathbb{F}_2^\ell)$$

$$= \Gamma \cdot \alpha^{i-1} \quad (\in \mathbb{F}_{2^\ell})$$

$$i = \log_\alpha(\boldsymbol{g_i}) - \log_\alpha(\Gamma) + 1$$

can be efficiently computed by Shor's algorithm for discrete log

Multiplying $M^\top$ corresponds to multiplying the generator α of $(\mathbb{F}_{2^\ell})^\times$

Attack Idea in Q2

$c := \mathrm{Cor}(\boldsymbol{s}^{(0)}G, \boldsymbol{z})$

NTT

1. ~~Collect the key stream $\boldsymbol{z} = (z_0, \ldots, z_{N-1})$ and store it into qRAM (after applying some linear transform)~~
2. Prepare the state corresponding to the function Ψ, i.e.,

$$|\psi\rangle := \frac{1}{\sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{w}} \Psi(\boldsymbol{w}) |\boldsymbol{w}\rangle$$

$\mathrm{poly}(\ell)$
by applying <u>Shor's algorithm</u>

3. Apply the Hadamard operator to obtain

$O(1)$

$$H^{\otimes \ell} |\psi\rangle = \frac{N}{2^{\ell} \cdot \sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{x}} \mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z}) |\boldsymbol{x}\rangle$$

4. Amplify the amplitude of $\boldsymbol{x}$ with a large $\mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})$ (with QAA)

$\mathrm{poly}(\ell) \cdot c^{-1}(c^{-1} + (\text{Step 2} + \text{Step 3}))$
by applying quantum counting

Attack Idea in Q2

$c := \mathrm{Cor}(\boldsymbol{s}^{(0)}G, \boldsymbol{z})$

NTT

1. ~~Collect the key stream $\boldsymbol{z} = (z_0, \ldots, z_{N-1})$ and store it into qRAM (after applying some linear transform)~~

2. Prepare the state corresponding to the function Ψ, i.e.,

$$|\psi\rangle := \frac{1}{\sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{w}} \Psi(\boldsymbol{w})|\boldsymbol{w}\rangle$$

$\mathrm{poly}(\ell)$

by applying Shor's algorithm

3. Apply the Hadamard operator to obtain

$O(1)$

$$H^{\otimes \ell}|\psi\rangle = \frac{N}{2^{\ell} \cdot \sqrt{\sum |\Psi(w)|^2}} \sum_{\boldsymbol{x}} \mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})|\boldsymbol{x}\rangle$$

4. Amplify the amplitude of $\boldsymbol{x}$ with a large $\mathrm{Cor}(\boldsymbol{x}G, \boldsymbol{z})$ (with QAA)

$\boxed{\textbf{Overall: } O\left(\ell^4 \cdot c^{-2}\right)}$

$\mathrm{poly}(\ell) \cdot c^{-1}(c^{-1} + (\text{Step 2} + \text{Step 3}))$

by applying quantum counting

Applications

Target	Key Length	Attack Model	Time	Data/Query	Ref./Note
SNOW 2.0	128 or 256	Classical	$2^{162.86}$	$2^{159.62}$	[GZ21]
		Q2	$2^{89.3}$	$2^{59.3}$	**This paper**
SNOW 3G	128	Classical	$2^{174.95}$	$2^{170.81}$	[GHW24]
		Q2	$2^{102.9}$	$2^{72.9}$	**This paper**
Sosemanuk	128 - 256	Classical	$2^{134.8}$	2^{135}	[ZLGJ23]
		Q1	2^{88}	$2^{7.46}$	[DWZS24]
		Q2	$2^{101.11}$	$2^{73.15}$	**This paper**

Any	k	Classical	2^k	k	Brute force
		Q1 or Q2	$2^{k/2}$	k	Grover search

Concurrent and Independent Work

A recent workshop abstract by Einsele and Wunder also mentions quantum speed-up of fast correlation attacks, but attack models and attack algorithms are not explained.

Summary

- Quantum algorithms on fast correlation attacks by relating classical FFT (FWHT) with QFT (Hadamard operator)
- In Q1, it seems hard to achieve meaningful speed-up
- In Q2, introducing a special attack model, an interesting speed-up is obtained by using Shor's alg. for discrete log
- Complexity in Q2 is $O(\ell^4/c^2)$ for ℓ-bit LFSR, if a linear approximation of correlation c is available
- First quantum attack on SNOW 2.0 faster than Grover and current best (quantum) fast correlation attack on SNOW 3G

Thank you!