# Legendre PRF (Multiple) Key Attacks and the Power of Preprocessing

Alexander May[1] Floyd Zweydinger[1]

10th August 2022

[1]Ruhr University Bochum, Germany

## Overview

Definition

Algorithms

- Single Key Attack With Preprocessing
- Multiple Key Attack With Preprocessing
- Multiple Key Attack Without Preprocessing

## Motivation

- Application in the Blockchain world
  - Ethereum 2.0
- Application Multi-Party-Computation
- Signature scheme: LegRoast
- Interesting PRF needs analysis

# Definition

# Legendre Symbol

## Definition (Legendre Symbol)

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \text{ is a quadratic residue} \\ -1 & \text{else.} \end{cases}$$

# Legendre Symbol

## Definition (Legendre Symbol)

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \text{ is a quadratic residue} \\ -1 & \text{else.} \end{cases}$$

## Definition (*Legendre PRF*)

For $k \in \mathbb{F}_p$:

$$\overline{L}_k : \mathbb{F}_p \to \{-1, 0, 1\} \text{ with } \overline{L}_k(x) = \left(\frac{x+k}{p}\right)$$

## Properties

- for all $x \in \mathbb{F}_p$

$$\overline{L}_k(x) = \overline{L}_0(x + k)$$

## Properties

- for all $x \in \mathbb{F}_p$

$$\overline{L}_k(x) = \overline{L}_0(x + k)$$

- if $y = k + x \Rightarrow \overline{L}_k(x) = \overline{L}_0(y)$

## Properties

- for all $x \in \mathbb{F}_p$

$$\overline{L}_k(x) = \overline{L}_0(x + k)$$

- if $y = k + x \Rightarrow \overline{L}_k(x) = \overline{L}_0(y)$
- When $\overline{L}_k(x) = \overline{L}_0(y) \Rightarrow y = k + x$ ?

## Legendre Points

**Definition (Legendre point)**

Set $r = \lceil 3 \log p \rceil$

$$L_k : \mathbb{F}_p \to \{-1, 0, 1\}^r,\ x \mapsto \left(\left(\frac{x+k}{p}\right), \ldots, \left(\frac{x+k+r-1}{p}\right)\right)$$

Denote $L = L_0$

# Legendre Points

## Definition (Legendre point)

Set $r = \lceil 3 \log p \rceil$

$$L_k : \mathbb{F}_p \to \{-1, 0, 1\}^r,\ x \mapsto \left(\left(\frac{x+k}{p}\right), \ldots, \left(\frac{x+k+r-1}{p}\right)\right)$$

Denote $L = L_0$

## Lemma

*Let $x, y \in \mathbb{F}_p$, then*

$$L(y) = L_k(x) \ \Rightarrow\ y = x + k$$

## Random Walk

- random function $f : \{-1, 0, 1\}^r \to \mathbb{F}_p$

## Random Walk

- random function $f : \{-1, 0, 1\}^r \to \mathbb{F}_p$
- *key-independent* random walk $W$ starts with $y^{(1)} \in_R \mathbb{F}_p$:

$$y^{(i+1)} = y^{(i)} + f\left(L\left(y^{(i)}\right)\right) \bmod p$$

## Random Walk

- random function $f : \{-1, 0, 1\}^r \to \mathbb{F}_p$
- *key-independent* random walk $W$ starts with $y^{(1)} \in_R \mathbb{F}_p$:

$$y^{(i+1)} = y^{(i)} + f\left(L\left(y^{(i)}\right)\right) \bmod p$$

- *key-dependent* random walk $\overline{W}_k$ starts with $x^{(1)} \in_R \mathbb{F}_p$:

$$x^{(i+1)} = x^{(i)} + f\left(L_k\left(x^{(i)}\right)\right) \bmod p$$

## Previous Work

- collision search by Khovratovich in $\mathcal{O}(\sqrt{p})$

## Previous Work

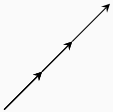
- collision search by Khovratovich in $\mathcal{O}(\sqrt{p})$

## Previous Work

- collision search by Khovratovich in $\mathcal{O}(\sqrt{p})$

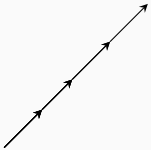
## Previous Work

- collision search by Khovratovich in $\mathcal{O}(\sqrt{p})$



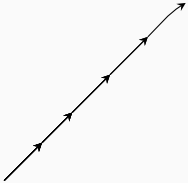
## Previous Work

- collision search by Khovratovich in $\mathcal{O}(\sqrt{p})$



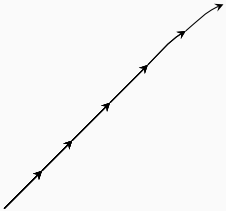
## Previous Work

- collision search by Khovratovich in $\mathcal{O}(\sqrt{p})$



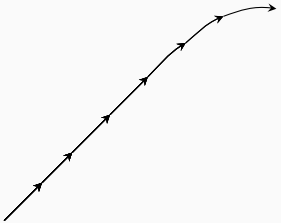
## Previous Work

- collision search by Khovratovich in $\mathcal{O}(\sqrt{p})$



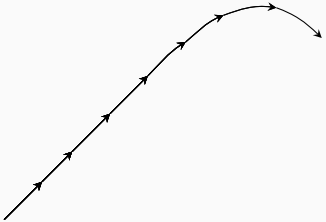
## Previous Work

- collision search by Khovratovich in $\mathcal{O}(\sqrt{p})$



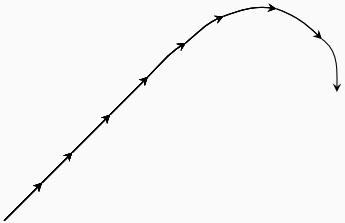
## Previous Work

- collision search by Khovratovich in $\mathcal{O}(\sqrt{p})$



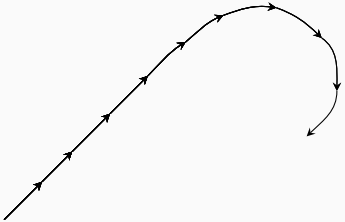
## Previous Work

- collision search by Khovratovich in $\mathcal{O}(\sqrt{p})$



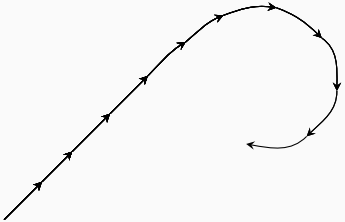
## Previous Work

- collision search by Khovratovich in $\mathcal{O}(\sqrt{p})$



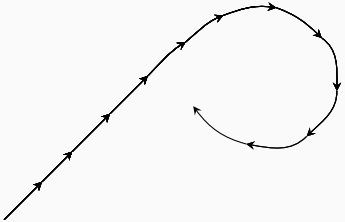
## Previous Work

- collision search by Khovratovich in $\mathcal{O}(\sqrt{p})$



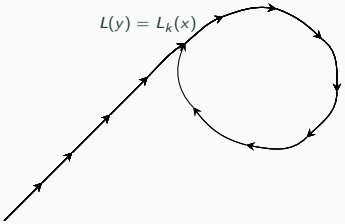
## Previous Work

- collision search by Khovratovich in $\mathcal{O}(\sqrt{p})$



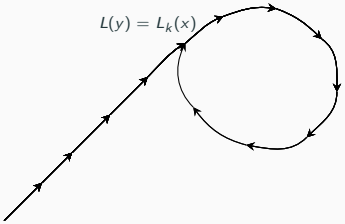
## Previous Work

- collision search by Khovratovich in $\mathcal{O}(\sqrt{p})$



## Previous Work

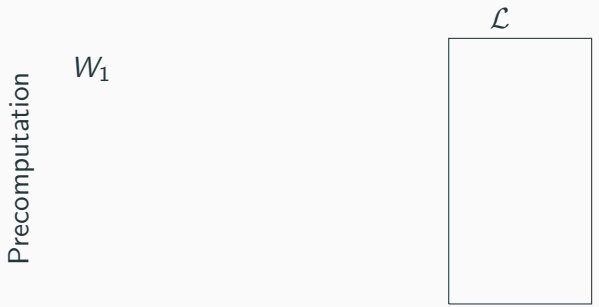
- collision search by Khovratovich in $\mathcal{O}(\sqrt{p})$




- polynomial improvements by Kaluđerović, Kleinjung, Kostić
- Goal: beat the $\sqrt{p}$ bound

# Algorithms

# Single Key Attack With Preprocessing

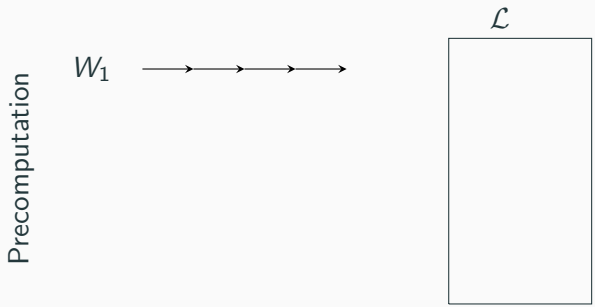


# Single Key Attack With Preprocessing

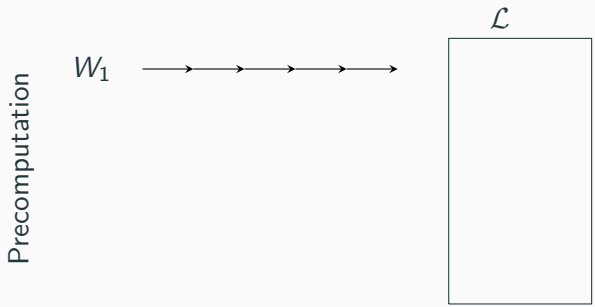
# Single Key Attack With Preprocessing

# Single Key Attack With Preprocessing

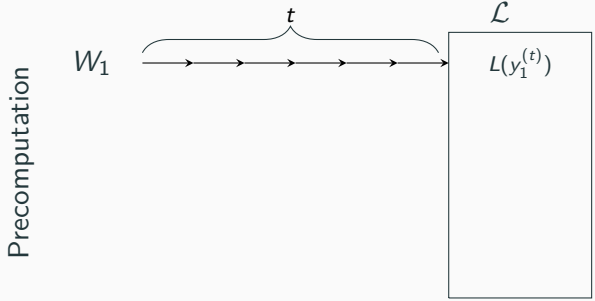
# Single Key Attack With Preprocessing



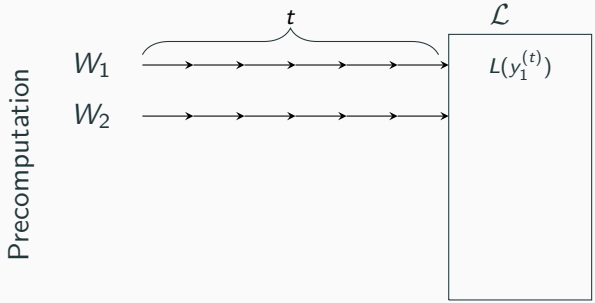
# Single Key Attack With Preprocessing



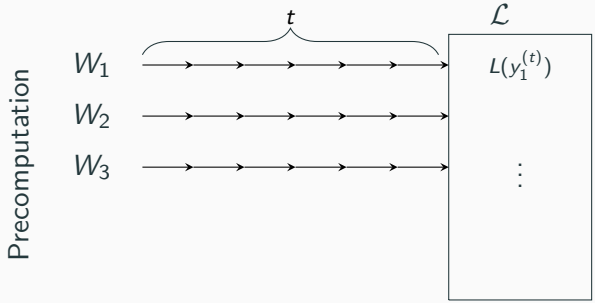
# Single Key Attack With Preprocessing



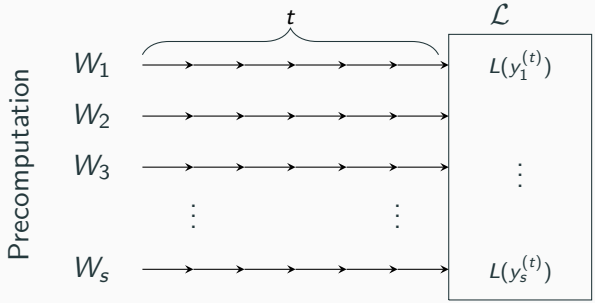
# Single Key Attack With Preprocessing



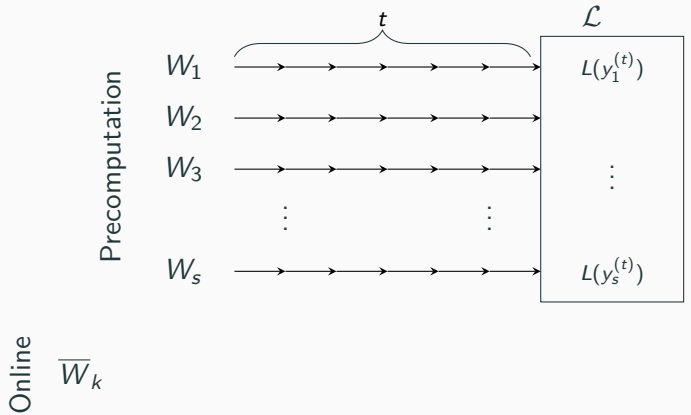
# Single Key Attack With Preprocessing



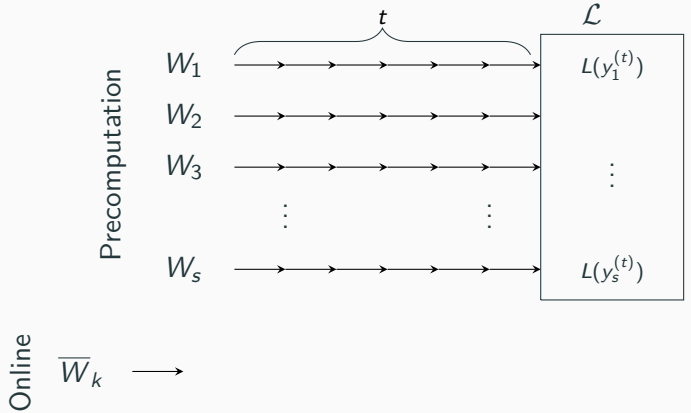
# Single Key Attack With Preprocessing



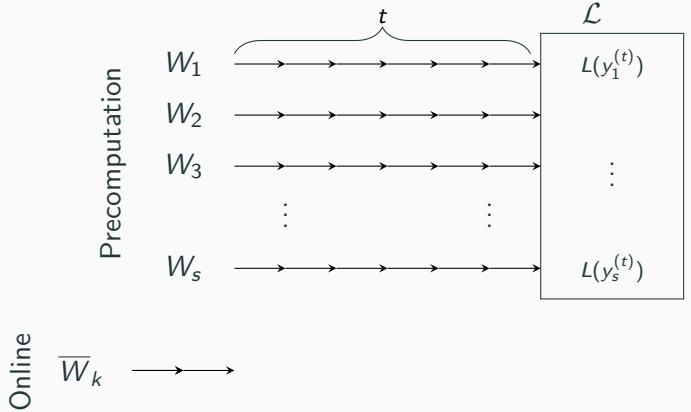
# Single Key Attack With Preprocessing



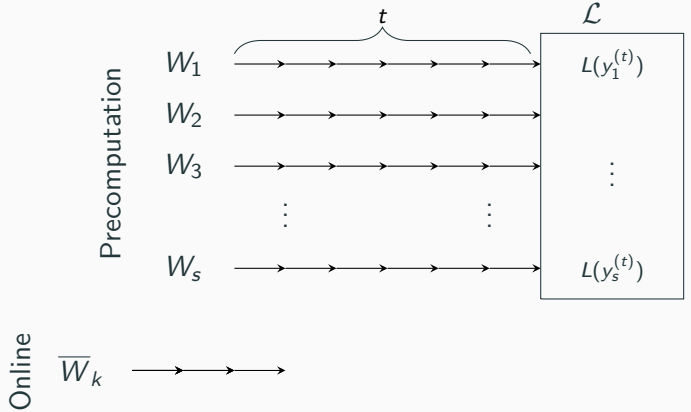
# Single Key Attack With Preprocessing



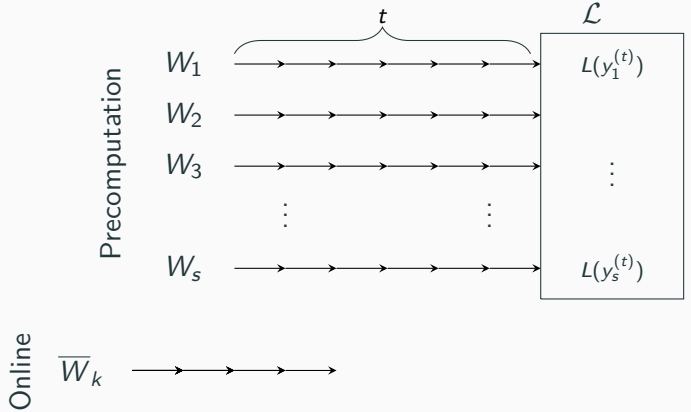
# Single Key Attack With Preprocessing



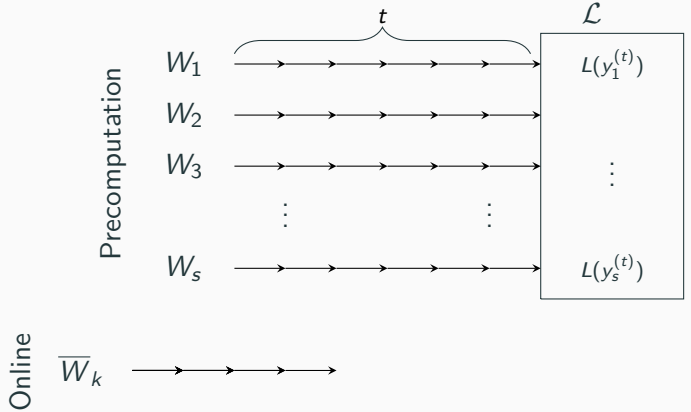
# Single Key Attack With Preprocessing



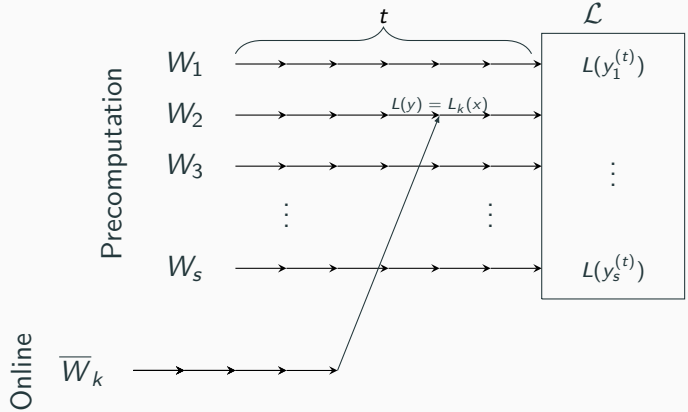
# Single Key Attack With Preprocessing



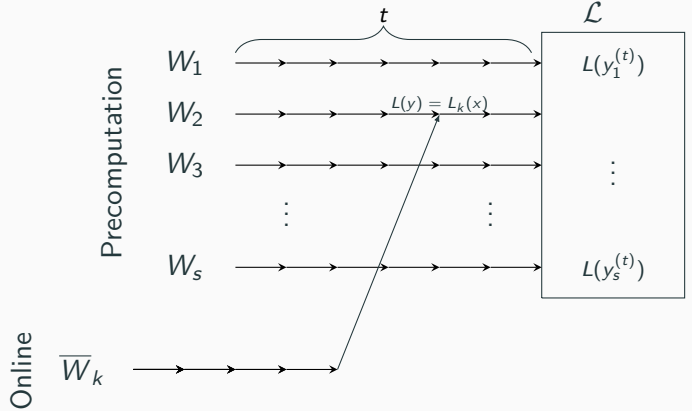
# Single Key Attack With Preprocessing



# Single Key Attack With Preprocessing



# Single Key Attack With Preprocessing




$$L(y) = L_k(x) \Rightarrow k = y - x \bmod p$$

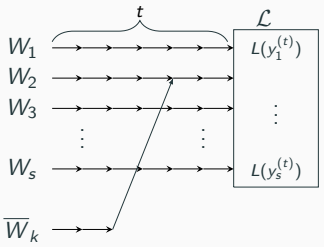
# Single Key Attack With Preprocessing: Analysis

**Theorem**

*The algorithm finds $k$*

*with precomputation time $\mathcal{O}(st)$ and online time $\mathcal{O}(t)$,*

$$\text{with probability } \Omega\left(\frac{st^2}{p}\right) \text{ and space } \mathcal{O}(s)$$



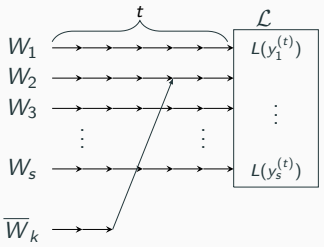
# Single Key Attack With Preprocessing: Analysis

**Theorem**

*The algorithm finds $k$*

*with precomputation time $\mathcal{O}(st)$ and online time $\mathcal{O}(t)$,*

$$\text{with probability } \Omega\left(\frac{st^2}{p}\right) \text{ and space } \mathcal{O}(s)$$

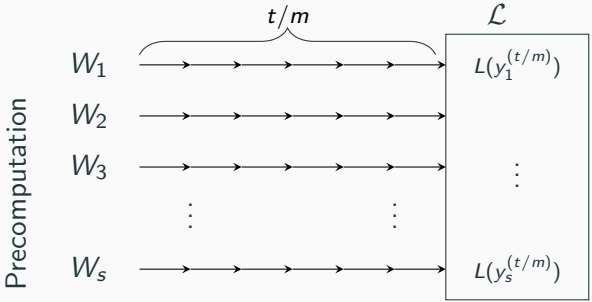



**Example**

$s = t = p^{1/3} \rightarrow$ precomputation time $= \mathcal{O}(p^{2/3})$, online time $= \mathcal{O}(p^{1/3})$

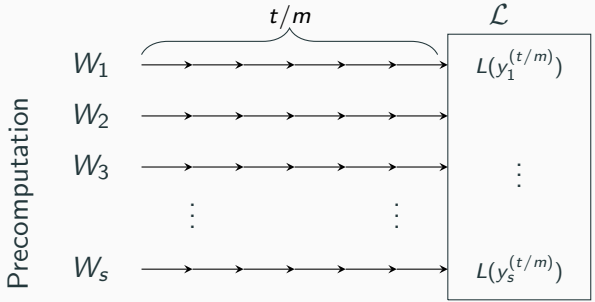
# Multiple Key Attack With Preprocessing

$m = \#keys$



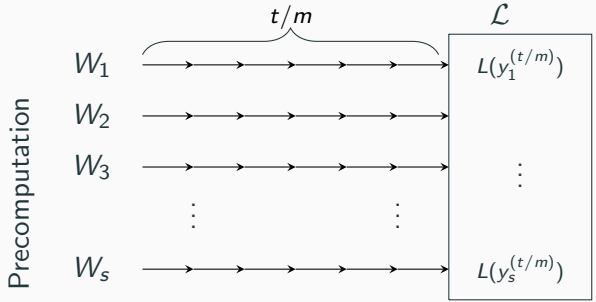
# Multiple Key Attack With Preprocessing

$m = \#keys$



# Multiple Key Attack With Preprocessing

$m = \#keys$

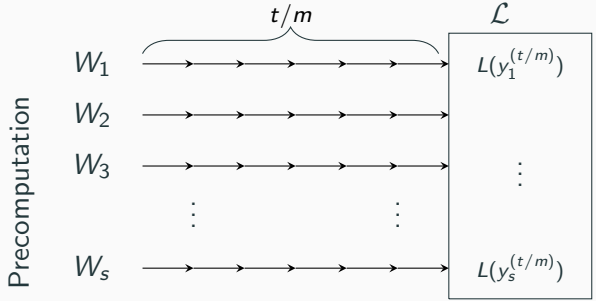



Online

$\overline{W}_{k_1}$

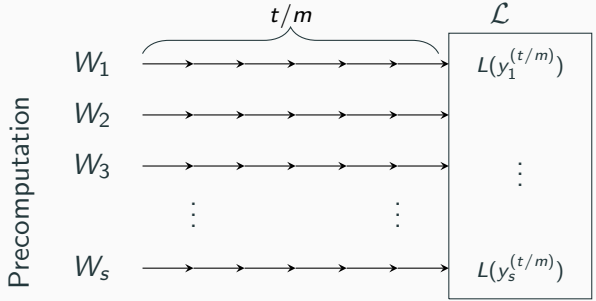
# Multiple Key Attack With Preprocessing

$m = \#keys$



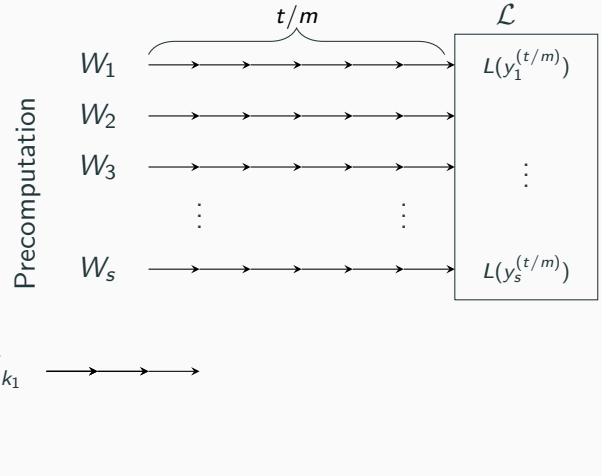
# Multiple Key Attack With Preprocessing

$m = \#keys$



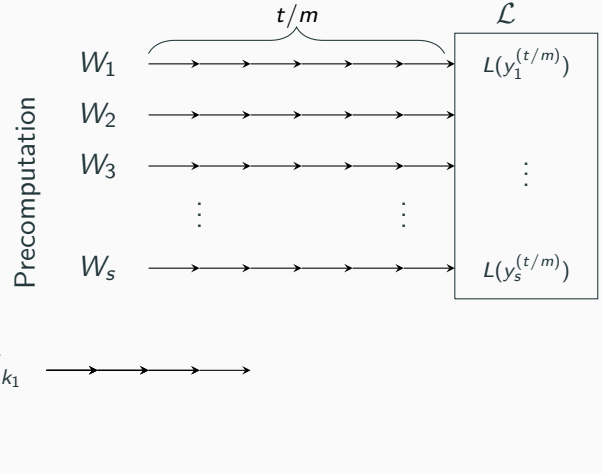
# Multiple Key Attack With Preprocessing

$m = \#keys$



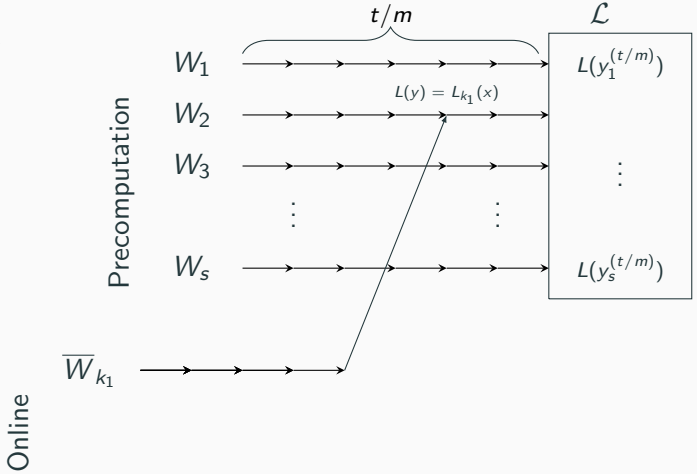
# Multiple Key Attack With Preprocessing

$m = \#keys$



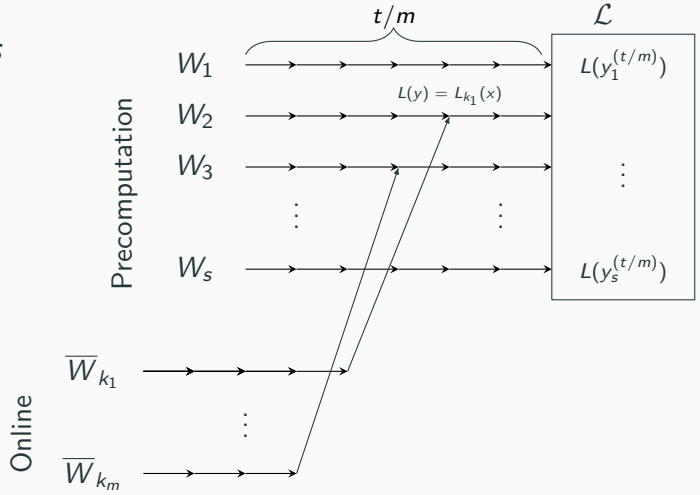
# Multiple Key Attack With Preprocessing

$m = \#keys$



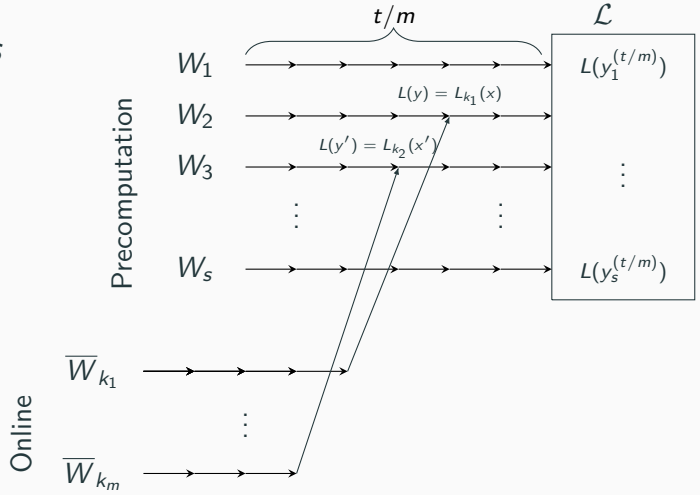
# Multiple Key Attack With Preprocessing

$m = \#keys$



# Multiple Key Attack With Preprocessing

$m = \#keys$



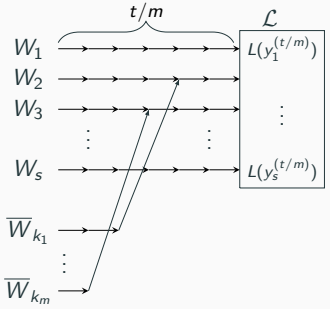
# Analysis

## Theorem

*The algorithm finds* $k_1, \ldots, k_m$

$$\text{with precomputation time } \mathcal{O}\left(\frac{st}{m}\right) \text{ and online time } \mathcal{O}(t),$$

$$\text{with probability } \Omega\left(\frac{st^2}{m^2 p}\right) \text{ and space } \mathcal{O}(s)$$



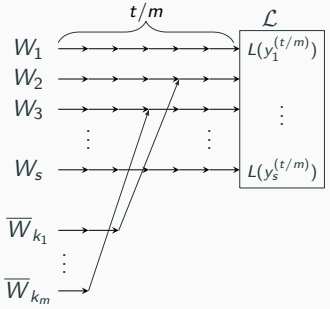
# Analysis

## Theorem

*The algorithm finds* $k_1, ..., k_m$

$$\text{with precomputation time } \mathcal{O}\left(\frac{st}{m}\right) \text{ and online time } \mathcal{O}(t),$$

$$\text{with probability } \Omega\left(\frac{st^2}{m^2 p}\right) \text{ and space } \mathcal{O}(s)$$




## Example

$$s = m^2 p^{1/3}, t = p^{1/3} \rightarrow \text{ precomputation in: } \mathcal{O}(m^2 p^{2/3}), \qquad \text{online in: } \mathcal{O}(p^{1/3})$$

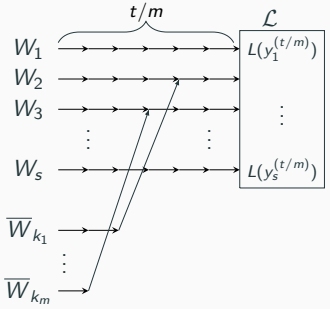
# Analysis

## Theorem

*The algorithm finds* $k_1, ..., k_m$

$$\text{with precomputation time } \mathcal{O}\left(\frac{st}{m}\right) \text{ and online time } \mathcal{O}(t),$$

$$\text{with probability } \Omega\left(\frac{st^2}{m^2 p}\right) \text{ and space } \mathcal{O}(s)$$

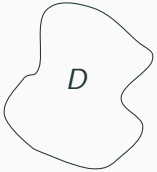



## Example

$$s = m^2 p^{1/3}, t = p^{1/3} \rightarrow \text{ precomputation in: } \mathcal{O}(m^2 p^{2/3}), \quad \text{online in: } \mathcal{O}(p^{1/3})$$

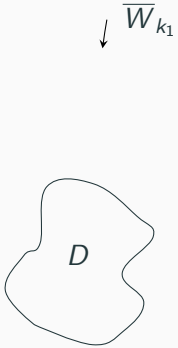
$$m = p^{1/6}, s = p^{1/3}, t = p^{1/2} \rightarrow \text{ precomputation in: } \mathcal{O}(p^{2/3}), \quad \text{online in: } \mathcal{O}(p^{1/2})$$

# Multiple Key Attack Without Preprocessing



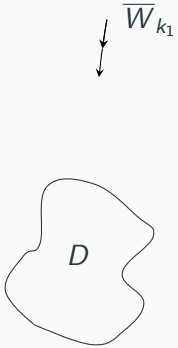

Set of Distinguished Points $D \subset \{-1, 0, 1\}^r$

# Multiple Key Attack Without Preprocessing



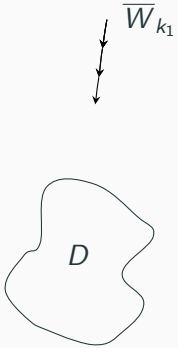

Set of Distinguished Points $D \subset \{-1, 0, 1\}^r$

# Multiple Key Attack Without Preprocessing



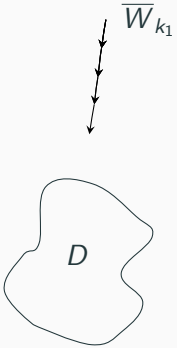

Set of Distinguished Points $D \subset \{-1, 0, 1\}^r$

# Multiple Key Attack Without Preprocessing



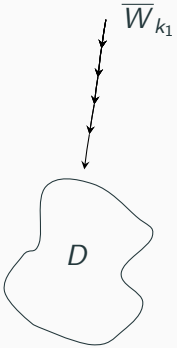

Set of Distinguished Points $D \subset \{-1, 0, 1\}^r$

# Multiple Key Attack Without Preprocessing



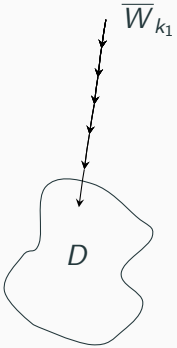

Set of Distinguished Points $D \subset \{-1, 0, 1\}^r$

# Multiple Key Attack Without Preprocessing




Set of Distinguished Points $D \subset \{-1, 0, 1\}^r$

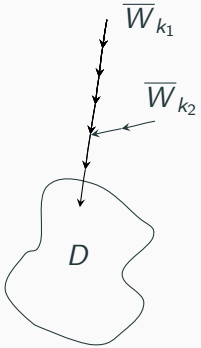
# Multiple Key Attack Without Preprocessing




Set of Distinguished Points $D \subset \{-1, 0, 1\}^r$

# Multiple Key Attack Without Preprocessing

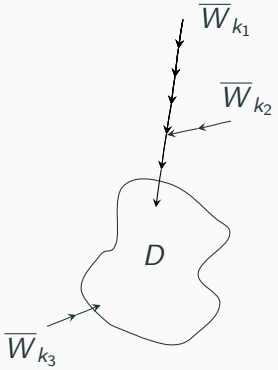
$$k_1 + x = k_2 + x'$$




Set of Distinguished Points $D \subset \{-1, 0, 1\}^r$

# Multiple Key Attack Without Preprocessing

$k_1 + x = k_2 + x'$

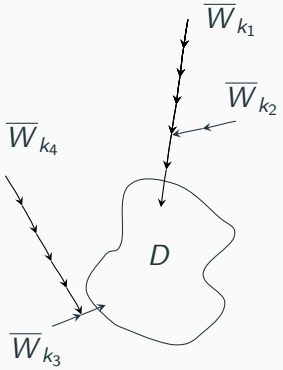



Set of Distinguished Points $D \subset \{-1, 0, 1\}^r$

# Multiple Key Attack Without Preprocessing

$$k_1 + x = k_2 + x'$$

$$k_3 + y = k_4 + y'$$



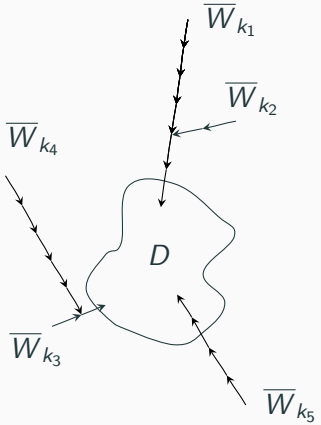

Set of Distinguished Points $D \subset \{-1, 0, 1\}^r$

# Multiple Key Attack Without Preprocessing

$$k_1 + x = k_2 + x'$$

$$k_3 + y = k_4 + y'$$

$$\dots$$



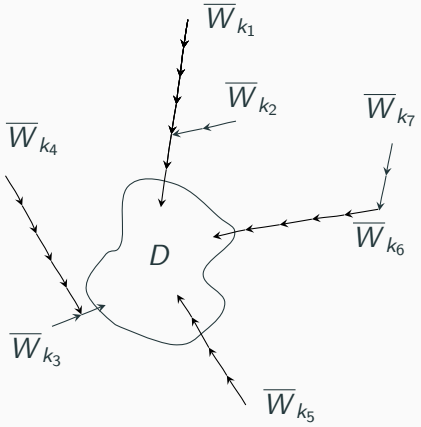

Set of Distinguished Points $D \subset \{-1, 0, 1\}^r$

# Multiple Key Attack Without Preprocessing

$$k_1 + x = k_2 + x'$$

$$k_3 + y = k_4 + y'$$

$$\dots$$

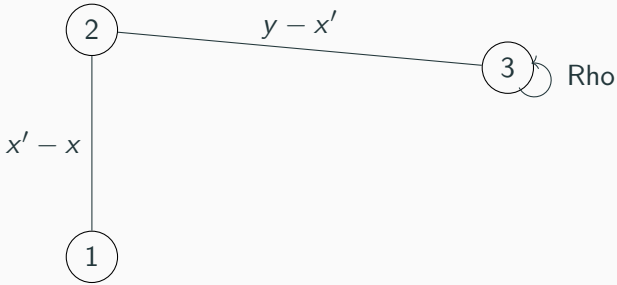



Set of Distinguished Points $D \subset \{-1, 0, 1\}^r$

# Graph Construction

$k_1 - k_2 = x' - x \bmod p$

$k_2 - k_3 = y - x' \bmod p$



# Multiple Key Attack Without Preprocessing: Analysis

**Theorem**

*The algorithm finds the keys $k_1, ..., k_m$ in time*

$$\mathcal{O}\left(\sqrt{mp}\right)$$

# Multiple Key Attack Without Preprocessing: Analysis

**Theorem**

*The algorithm finds the keys $k_1, \ldots, k_m$ in time*

$$\mathcal{O}\left(\sqrt{mp}\right)$$

*Amortized for each key*

$$\mathcal{O}\left(\frac{\sqrt{p}}{\sqrt{m}}\right)$$

## Results

- 3 different algorithms attacking the Legendre PRF
- we can beat $\mathcal{O}(\sqrt{p})$ if:

## Results

- 3 different algorithms attacking the Legendre PRF
- we can beat $\mathcal{O}(\sqrt{p})$ if:
  - preprocessing is used

## Results

- 3 different algorithms attacking the Legendre PRF
- we can beat $\mathcal{O}(\sqrt{p})$ if:
  - preprocessing is used
  - many keys are attacked

## Results

- 3 different algorithms attacking the Legendre PRF
- we can beat $\mathcal{O}(\sqrt{p})$ if:
  - preprocessing is used
  - many keys are attacked

Thank You!

eprint: `https://eprint.iacr.org/2021/645`

code: `https://github.com/FloydZ/prep-legendre`