The Iterated Random Function Problem
ASK 2016, Nagoya, Japan

Mridul Nandi

Indian Statistical Institute, Kolkata

28 September 2016
Joint work with Ritam Bhaumik, Nilanjan Datta, Avijit Dutta, Ashwin Jha, Avradip Mandal, Nicky Mouha.
Iterated Random Function

Outline of the Talk

- Iterated random function
Outline of the Talk

- Iterated random function
- Known vs. Our Approach
Outline of the Talk

- Iterated random function
- Known vs. Our Approach
- Types of Collision for (iterated) random function
Outline of the Talk

- Iterated random function
- Known vs. Our Approach
- Types of Collision for (iterated) random function
- Collision Probabilities and PRF analysis
Fix a positive integer $r$, and a random permutation $f$. Minaud and Seurin in crypto 2015 studied PRP of $f^r = f \circ \cdots \circ f$ ($r$ times) with $O\left(\frac{rq}{2^n}\right)$ PRP advantage. Lower bound of PRP advantage is sometimes $\Theta\left(\frac{q}{2^n}\right)$. Scope of improvement...
Fix a positive integer $r$, and a random permutation $f$. 

Minaud and Seurin in crypto 2015 studied PRP of $f^r = f \circ \cdots \circ f$ (r times) 

$O\left(\frac{rq}{2n}\right)$ PRP advantage

Lower bound of PRP advantage sometimes $\Theta\left(\frac{q}{2n}\right)$
The Iterated Random Permutations Problem

- Fix a positive integer $r$, and a random permutation $f$.
- Minaud and Seurin in crypto 2015 studied PRP of $f^r = f \circ \cdots \circ f$ ($r$ times)
The Iterated Random Permutations Problem

- Fix a positive integer $r$, and a random permutation $f$.
- Minaud and Seurin in crypto 2015 studied PRP of
  $f^r = f \circ \cdots \circ f$ ($r$ times)
- $O(rq/2^n)$ PRP advantage
The Iterated Random Permutations Problem

- Fix a positive integer $r$, and a random permutation $f$.

- Minaud and Seurin in crypto 2015 studied PRP of $f^r = f \circ \cdots \circ f$ ($r$ times)

- $O(rq/2^n)$ PRP advantage

- Lower bound of PRP advantage sometimes $\Theta(q/2^n)$
The Iterated Random Permutations Problem

- Fix a positive integer $r$, and a random permutation $f$.
- Minaud and Seurin in crypto 2015 studied PRP of $f^r = f \circ \cdots \circ f$ ($r$ times)
- $O(rq/2^n)$ PRP advantage
- Lower bound of PRP advantage sometimes $\Theta(q/2^n)$
- Scope of improvement
The Iterated Random Function Problem

- We ask same problem for random function
The Iterated Random Function Problem

- We ask the same problem for random function
- We show $\Theta(rq^2/2^n)$ PRF advantage
The Iterated Random Function Problem

- We ask same problem for random function
- We show $\Theta(\frac{rq^2}{2^n})$ PRF advantage
- We show an attack with advantage about $\frac{rq^2}{2^n}$ provided $q \geq 2^{n/3}$
The Iterated Random Function Problem

- We ask same problem for random function
- We show $\Theta(rq^2/2^n)$ PRF advantage
- We show an attack with advantage about $rq^2/2^n$ provided $q \geq 2^{n/3}$
- We show upper bound using Coefficients H Technique
Known Approach: Full Collision Probability

- Used for analyzing Improved bound of CBC by Bellare, Pietrzak and Rogaway in crypto 2005
Known Approach: Full Collision Probability

- Used for analyzing Improved bound of CBC by Bellare, Pietrzak and Rogaway in crypto 2005
- $O(rq^2/2^n)$ PRF advantage for CBC of length $r$
Known Approach: Full Collision Probability

- Used for analyzing Improved bound of CBC by Bellare, Pietrzak and Rogaway in crypto 2005
- $O(rq^2/2^n)$ PRF advantage for CBC of length $r$
- Collision between a final input ($q$ such) and other $rq$ inputs
Known Approach: Full Collision Probability

- Used for analyzing Improved bound of CBC by Bellare, Pietrzak and Rogaway in crypto 2005
- $O(rq^2/2^n)$ PRF advantage for CBC of length $r$
- Collision between a final input ($q$ such) and other $rq$ inputs
- On the average $1/2^n$ collision probability for a pair
Known Approach: Full Collision Probability

- Used for analyzing Improved bound of CBC by Bellare, Pietrzak and Rogaway in crypto 2005
- $O(rq^2/2^n)$ PRF advantage for CBC of length $r$
- Collision between a final input ($q$ such) and other $rq$ inputs
- On the average $1/2^n$ collision probability for a pair
- Unfortunately this is not true for random function (collision probability for a pair can be $O(rq/2^n)$)
Our Approach: Upper Bound
Our Approach: Upper Bound

- Allow all collisions on $f$ that do not lead to collision on $f^r$
Our Approach: Upper Bound

- Allow all collisions on $f$ that do not lead to collision on $f^r$
- Look at possible function graphs of $f$ and $f^r$
Our Approach: Upper Bound

- Allow *all* collisions on $f$ that do not lead to collision on $f^r$
- Look at possible function graphs of $f$ and $f^r$
- Bound probabilities of different types of collisions
Our Approach: Upper Bound

- Allow all collisions on $f$ that do not lead to collision on $f^r$
- Look at possible function graphs of $f$ and $f^r$
- Bound probabilities of different types of collisions
- Use Coefficient H Technique to upper bound advantage
Our Approach : Lower Bound

- We show lower bound
Our Approach : Lower Bound

- We show lower bound
- Vary first block and rest all blocks are same
Our Approach: Lower Bound

- We show lower bound
- Vary first block and rest all blocks are same
- For a pair collision probability about $r/2^n$
Our Approach: Lower Bound

- We show lower bound
- Vary first block and rest all blocks are same
- For a pair collision probability about $r/2^n$
- Use Inclusion Exclusion Principle to lower bound advantage
Our Approach: Lower Bound

- We show lower bound
- Vary first block and rest all blocks are same
- For a pair collision probability about $r/2^n$
- Use Inclusion Exclusion Principle to lower bound advantage
- So it is tight up to a small power of log $r$
Function Graphs

- Views function as directed graph $y = f(x)$ represented by an edge from $x$ to $y$.
- Loops allowed, no multiple edges.
- Trails move together once merged.
- All trails eventually lead to cycles.
Function Graphs

- Views function as directed graph
Function Graphs

- Views function as directed graph
- $y = f(x)$ represented by an edge from $x$ to $y$
Function Graphs

- Views function as directed graph
- \( y = f(x) \) represented by an edge from \( x \) to \( y \)
- Loops allowed, no multiple edges
Function Graphs

- Views function as directed graph
- \( y = f(x) \) represented by an edge from \( x \) to \( y \)
- Loops allowed, no multiple edges
- Trails move together once merged
Function Graphs

- Views function as directed graph
- $y = f(x)$ represented by an edge from $x$ to $y$
- Loops allowed, no multiple edges
- Trails move together once merged
- All trails eventually lead to cycles
Collision Attack on $f$

Two main approaches:
Collision Attack on $f$

Two main approaches:

- **Feedback Attack:**

  - $x_i$, query $i$:
  
  

  Tries to find cycle

  - Multiple Trails Attack:

    - $x_j$, query $i$ on Trail $j$:
      
  Tries to make two trails merge
Collision Attack on $f$

Two main approaches:

- **Feedback Attack:**
  - Based on Pollard’s Rho Algorithm
Collision Attack on $f$

Two main approaches:

- **Feedback Attack**:  
  - Based on Pollard’s Rho Algorithm  
  - Keeps feeding back $f$'s outputs to $f$
Collision Attack on $f$

Two main approaches:

- **Feedback Attack:**
  - Based on Pollard’s Rho Algorithm
  - Keeps feeding back $f$’s outputs to $f$
  - Query 1: $x$, query $i$: $f^{i-1}(x)$
Collision Attack on $f$

Two main approaches:

- **Feedback Attack:**
  - Based on Pollard’s Rho Algorithm
  - Keeps feeding back $f$’s outputs to $f$
  - Query 1: $x$, query $i$: $f^{i-1}(x)$
  - Tries to find cycle
Collision Attack on $f$

Two main approaches:

- **Feedback Attack:**
  - Based on Pollard’s Rho Algorithm
  - Keeps feeding back $f$’s outputs to $f$
  - Query 1: $x$, query $i$: $f^{i-1}(x)$
  - Tries to find cycle

- **Multiple Trails Attack:**
Collision Attack on $f$

Two main approaches:

- **Feedback Attack:**
  - Based on Pollard’s Rho Algorithm
  - Keeps feeding back $f$’s outputs to $f$
  - Query 1: $x$, query $i$: $f^{i-1}(x)$
  - Tries to find cycle

- **Multiple Trails Attack:**
  - Based loosely on van Oorschot-Wiener’s Parallel Search
Collision Attack on $f$

Two main approaches:

- **Feedback Attack:**
  - Based on Pollard’s Rho Algorithm
  - Keeps feeding back $f$’s outputs to $f$
  - Query 1: $x$, query $i$: $f^{i-1}(x)$
  - Tries to find cycle

- **Multiple Trails Attack:**
  - Based loosely on van Oorschot-Wiener’s Parallel Search
  - Starts feedback queries simultaneously from many points
Collision Attack on $f$

Two main approaches:

- **Feedback Attack:**
  - Based on Pollard’s Rho Algorithm
  - Keeps feeding back $f$’s outputs to $f$
  - Query 1: $x$, query $i$: $f^{i-1}(x)$
  - Tries to find cycle

- **Multiple Trails Attack:**
  - Based loosely on van Oorschot-Wiener’s Parallel Search
  - Starts feedback queries simultaneously from many points
  - Query 1 on Trail $j$: $x_j$, query $i$ on Trail $j$: $f^{i-1}(x_j)$
Collision Attack on $f$

Two main approaches:

- **Feedback Attack:**
  - Based on Pollard’s Rho Algorithm
  - Keeps feeding back $f$’s outputs to $f$
  - Query 1: $x$, query $i$: $f^{i-1}(x)$
  - Tries to find cycle

- **Multiple Trails Attack:**
  - Based loosely on van Oorschot-Wiener’s Parallel Search
  - Starts feedback queries simultaneously from many points
  - Query 1 on Trail $j$: $x_j$, query $i$ on Trail $j$: $f^{i-1}(x_j)$
  - Tries to make two trails merge
Collision Types on $f$
Collision Types on $f$

- **Rho collision**

![Diagram of Rho collision with labeled points and arrows indicating collision point, cycle length $c$, and two foot lengths $t_1$ and $t_2$.]
Collision Types on $f$

- **Rho collision**
  - Tail length $t$

Diagram:
- A cycle labeled $c$
- Two points $x_1$ and $x_2$ connected by lines $t$
- A collision point indicated with a red arrow
Collision Types on $f$

- **Rho collision**
  - Tail length $t$
  - Cycle length $c$

![Diagram of Rho collision](image)
Collision Types on $f$

- **Rho collision**
  - Tail length $t$
  - Cycle length $c$
  - Denoted $\rho(t, c)$
Collision Types on $f$

**Rho collision**
- Tail length $t$
- Cycle length $c$
- Denoted $\rho(t, c)$

**Lambda collision**
Collision Types on $f$

- **Rho collision**
  - Tail length $t$
  - Cycle length $c$
  - Denoted $\rho(t, c)$

- **Lambda collision**
  - Foot lengths $t_1$ and $t_2$
Iterated Random Function

Collision Types on $f$

- **Rho collision**
  - Tail length $t$
  - Cycle length $c$
  - Denoted $\rho(t, c)$

- **Lambda collision**
  - Foot lengths $t_1$ and $t_2$
  - Denoted $\lambda(t_1, t_2)$
Collision Probabilities on $f$

\[
\Pr[\rho(t, c)] \leq 1 - e^{-\alpha N}\quad \text{for } t = \Theta(\sqrt{\alpha N})
\]

\[
\Pr[\lambda(t_1, t_2)] \leq 1 - e^{-\alpha N}
\]
Collision Probabilities on $f$

- Rho collision

\[
\Pr[\rho(t, c)] \leq 1 - \alpha N \quad \text{for } t = \Theta(\sqrt{\alpha N})
\]

\[
\Pr[\lambda(t_1, t_2)] \leq 1 - e^{-\alpha N}
\]
Collision Probabilities on $f$

- **Rho collision**

- Feedback attack from some $x$

\[
\Pr[\rho(t, c)] \leq \frac{1}{N}
\]

\[
\Pr[\lambda(t_1, t_2)] \leq \frac{1}{N}
\]
Collision Probabilities on $f$

- **Rho collision**
  - Feedback attack from some $x$
  - $\Pr[\rho(t, c)] \leq \frac{1}{N}$
Collision Probabilities on $f$

- **Rho collision**
  - Feedback attack from some $x$
  - $\Pr [\rho(t, c)] \leq \frac{1}{N}$
  - $\Pr [\rho(t, c)] \leq \frac{e^{-\alpha}}{N}$ for $t = \Theta(\sqrt{\alpha N})$
Collision Probabilities on $f$

- **Rho collision**
  - Feedback attack from some $x$
  - $\Pr[\rho(t, c)] \leq \frac{1}{N}$
  - $\Pr[\rho(t, c)] \leq \frac{e^{-\alpha}}{N}$ for $t = \Theta(\sqrt{\alpha N})$

- **Lambda collision**
Collision Probabilities on $f$

- **Rho collision**
  - Feedback attack from some $x$
  - $\Pr[\rho(t, c)] \leq \frac{1}{N}$
  - $\Pr[\rho(t, c)] \leq \frac{e^{-\alpha}}{N}$ for $t = \Theta(\sqrt{\alpha N})$

- **Lambda collision**
  - Two-trail attack from some $x_1$ and $x_2$
Collision Probabilities on $f$

- **Rho collision**
  - Feedback attack from some $x$
  - $\Pr[\rho(t, c)] \leq \frac{1}{N}$
  - $\Pr[\rho(t, c)] \leq \frac{e^{-\alpha}}{N}$ for $t = \Theta(\sqrt{\alpha N})$

- **Lambda collision**
  - Two-trail attack from some $x_1$ and $x_2$
  - $\Pr[\lambda(t_1, t_2)] \leq \frac{1}{N}$
Collision Attack on $f^r$

Same two approaches:

**Feedback Attack:**
- Keeps feeding back $f^r$'s outputs to $f^r$
- Query 1: $x_i$, query $i$: $(f^r)_{i-1}(x)$
  - Tries to find cycle

**Multiple Trails Attack:**
- Starts feedback queries simultaneously from many points
- Query 1 on Trail $j$: $x_j$
- Query $i$ on Trail $j$: $(f^r)_{i-1}(x_j)$
  - Tries to make two trails merge
Collision Attack on $f'$

Same two approaches:

- **Feedback Attack:**

  Query 1:
  
  $x_i$:
  
  $f'_{i-1}(x_i)$

  Tries to find cycle

  Multiple Trails Attack:

  Starts feedback queries simultaneously from many points

  Query 1 on Trail $j$:
  
  $x_{j_i}$

  Query $i$ on Trail $j$:
  
  $f'_{i-1}(x_{j_i})$
Iterated Random Function

Collision Attack on $f^r$

Same two approaches:

- **Feedback Attack:**
  - Keeps feeding back $f^r$'s outputs to $f^r$
Collision Attack on $f^r$

Same two approaches:

- **Feedback Attack:**
  - Keeps feeding back $f^r$'s outputs to $f^r$
  - Query 1: $x$, query $i$: $(f^r)^{i-1}(x)$
Collision Attack on $f^r$

Same two approaches:

- **Feedback Attack:**
  - Keeps feeding back $f^r$'s outputs to $f^r$
  - Query 1: $x$, query $i$: $(f^r)^{i-1}(x)$
  - Tries to find cycle
Collision Attack on $f^r$

Same two approaches:

- **Feedback Attack:**
  - Keeps feeding back $f^r$'s outputs to $f^r$
  - Query 1: $x$, query $i$: $(f^r)^{i-1}(x)$
  - Tries to find cycle

- **Multiple Trails Attack:**
Collision Attack on $f^r$

Same two approaches:

- **Feedback Attack:**
  - Keeps feeding back $f^r$'s outputs to $f^r$
  - Query 1: $x$, query $i$: $(f^r)^i(x)$
  - Tries to find cycle

- **Multiple Trails Attack:**
  - Starts feedback queries simultaneously from many points
Collision Attack on $f^r$

Same two approaches:

- **Feedback Attack:**
  - Keeps feeding back $f^r$'s outputs to $f^r$
  - Query 1: $x$, query $i$: $(f^r)^{i-1}(x)$
  - Tries to find cycle

- **Multiple Trails Attack:**
  - Starts feedback queries simultaneously from many points
  - Query 1 on Trail $j$: $x_j$, query $i$ on Trail $j$: $(f^r)^{i-1}(x_j)$
Collision Attack on $f^r$

Same two approaches:

- **Feedback Attack:**
  - Keeps feeding back $f^r$'s outputs to $f^r$
  - Query 1: $x$, query $i$: $(f^r)^{i-1}(x)$
  - Tries to find cycle

- **Multiple Trails Attack:**
  - Starts feedback queries simultaneously from many points
  - Query 1 on Trail $j$: $x_j$, query $i$ on Trail $j$: $(f^r)^{i-1}(x_j)$
  - Tries to make two trails merge
Collision Types on $f^r$

Can be reduced to collisions on $f$:

Direct $\rho$ collision:

$\rho$-collision in phase with $r = t + c \mod r$

Delayed $\rho$ collision:

$\rho$-collision out of phase move around cycle $\eta$ times in all to adjust phase $\eta = r / \gcd(c, r)$

$t = t + c \eta \mod r$

Collision point
Collision Types on $f^r$

- Can be reduced to collisions on $f$
Collision Types on $f^r$

- Can be reduced to collisions on $f$
- **Rho collision:**

![Diagram of Rho collision]

**Collision point**

```math
\text{Rho collision:}
\begin{align*}
\text{Direct } \rho \text{ collision:} & \quad f^- \text{collision in phase with } r \\
\text{Delayed } \rho \text{ collision:} & \quad f^- \text{collision out of phase move around cycle } \eta \text{ times in all to adjust phase } \\
\eta & = \frac{r}{\gcd(c, r)} \\
t & = t + c \eta \mod r
\end{align*}
```
Collision Types on $f^r$

- Can be reduced to collisions on $f$
- **Rho collision:**
  - *Direct ρ collision:*
    
    - **Collision point**
      
      - $t = t + c \eta \mod r$
      - $\eta = r / \gcd(c, r)$
Collision Types on $f^r$

- Can be reduced to collisions on $f$

- **Rho collision:**
  - Direct $\rho$ collision:
    - $f$-collision in phase with $r$

```latex
collision point
```
```latex
t \rightarrow t + c \eta \mod r
```
```latex
x \rightarrow x + c \eta \mod r
```
Collision Types on $f^r$

- Can be reduced to collisions on $f$

- **Rho collision:**
  - **Direct $\rho$ collision:**
    - $f$-collision in phase with $r$
    - $t = t + c \mod r$

- \[\eta = r / \gcd(c, r)\]
- \[t = t + c \eta \mod r\]
Collision Types on $f^r$

- Can be reduced to collisions on $f$
- **Rho collision:**
  - *Direct $\rho$ collision:*
    - $f$-collision in phase with $r$
    - $t = t + c \mod r$
  - *Delayed $\rho$ collision:*

![Diagram](image.png)
Collision Types on $f^r$

- Can be reduced to collisions on $f$

- **Rho collision:**
  - *Direct $\rho$ collision:*
    - $f$-collision in phase with $r$
    - $t = t + c \mod r$
  - *Delayed $\rho$ collision:*
    - $f$-collision out of phase

[Diagram showing iteration and collision points]
Collision Types on $f^r$

- Can be reduced to collisions on $f$

- **Rho collision:**
  - *Direct $\rho$ collision:*
    - $f$-collision in phase with $r$
    - $t = t + c \mod r$
  - *Delayed $\rho$ collision:*
    - $f$-collision out of phase
    - move around cycle $\eta$ times in all to adjust phase

\[ \eta = \frac{r}{\gcd(c, r)} \]
\[ t = t + c \eta \mod r \]
Collision Types on $f^r$

- Can be reduced to collisions on $f$

**Rho collision:**

- **Direct $\rho$ collision:**
  - $f$-collision in phase with $r$
  - $t = t + c \mod r$

- **Delayed $\rho$ collision:**
  - $f$-collision out of phase
  - move around cycle $\eta$ times in all to adjust phase
  - $\eta = r / \gcd(c, r)$
Collision Types on $f^r$

- Can be reduced to collisions on $f$

**Rho collision:**

- *Direct $\rho$ collision:*
  - $f$-collision in phase with $r$
  - $t = t + c \mod r$

- *Delayed $\rho$ collision:*
  - $f$-collision out of phase
  - move around cycle $\eta$ times in all to adjust phase
  - $\eta = r / \gcd(c, r)$
  - $t = t + c\eta \mod r$
Collision Types on $f^r$

- Can be reduced to collisions on $f$

- **Lambda collision:**

  - Direct $\lambda$ collision: $f$-collision in phase with $t_1 = t_2 \mod r$
  
  - Delayed $\lambda$ collision: $f$-collision out of phase
    - Find $\rho$ collision on merged walk
    - Move around cycle $\eta$ times in all to adjust phase
    - $t_1 = t_2 + c \eta \mod r$
    
    - Also called $\lambda\rho$ collision or $\rho'$ collision

  - Needs 2 $f$-collisions
Collision Types on $f^r$

- Can be reduced to collisions on $f$

- **Lambda collision:**
  - *Direct $\lambda$ collision:*

![Diagram showing collision points and time intervals](image)
Collision Types on $f^r$

- Can be reduced to collisions on $f$
- **Lambda collision:**
  - **Direct $\lambda$ collision:**
    - $f$-collision in phase with $r$

![Diagram showing collision types](image)
Collision Types on $f^r$

- Can be reduced to collisions on $f$

- **Lambda collision:**
  - *Direct $\lambda$ collision:*
    - $f$-collision in phase with $r$
    - $t_1 = t_2 \mod r$

Diagram:
- Second collision point
- First collision point
- $\Delta t$
- $x_1, x_2$
- $t_1, t_2$
- $c$
Collision Types on $f^r$

- Can be reduced to collisions on $f$

**Lambda collision:**

- *Direct $\lambda$ collision:*
  - $f$-collision in phase with $r$
  - $t_1 = t_2 \text{ mod } r$

- *Delayed $\lambda$ collision:*
  - $\Delta t = \eta = \text{cycle length}$
  - $t_1 = t_2 + \Delta t \text{ mod } r$

![Diagram]

- Second collision point
- First collision point
- $\Delta t$
Collision Types on $f^r$

- Can be reduced to collisions on $f$

- **Lambda collision:**
  - *Direct $\lambda$ collision:*
    - $f$-collision in phase with $r$
    - $t_1 = t_2 \mod r$
  - *Delayed $\lambda$ collision:*
    - $f$-collision out of phase
Collision Types on $f^r$

- Can be reduced to collisions on $f$

- **Lambda collision:**
  - *Direct $\lambda$ collision:*
    - $f$-collision in phase with $r$
    - $t_1 = t_2 \mod r$
  - *Delayed $\lambda$ collision:*
    - $f$-collision out of phase
    - find $\rho$ collision on merged walk

![Diagram](image-url)
Collision Types on $f^r$

- Can be reduced to collisions on $f$

**Lambda collision:**

- **Direct $\lambda$ collision:**
  - $f$-collision in phase with $r$
  - $t_1 = t_2 \mod r$

- **Delayed $\lambda$ collision:**
  - $f$-collision out of phase
  - find $\rho$ collision on merged walk
  - move around cycle $\eta$ times in all to adjust phase
Collision Types on $f^r$

- Can be reduced to collisions on $f$

- **Lambda collision:**
  - Direct $\lambda$ collision:
    - $f$-collision in phase with $r$
    - $t_1 = t_2 \mod r$
  - Delayed $\lambda$ collision:
    - $f$-collision out of phase
    - Find $\rho$ collision on merged walk
    - Move around cycle $\eta$ times in all to adjust phase
    - $t_1 = t_2 + c\eta \mod r$
Collision Types on $f^r$

- Can be reduced to collisions on $f$

**Lambda collision:**

- **Direct $\lambda$ collision:**
  - $f$-collision in phase with $r$
  - $t_1 = t_2 \mod r$

- **Delayed $\lambda$ collision:**
  - $f$-collision out of phase
  - find $\rho$ collision on merged walk
  - move around cycle $\eta$ times in all to adjust phase
  - $t_1 = t_2 + c\eta \mod r$
  - also called $\lambda\rho$ collision or $\rho'$ collision
Collision Types on $f^r$

- Can be reduced to collisions on $f$

**Lambda collision:**

- **Direct $\lambda$ collision:**
  - $f$-collision in phase with $r$
  - $t_1 = t_2 \mod r$

- **Delayed $\lambda$ collision:**
  - $f$-collision out of phase
  - Find $\rho$ collision on merged walk
  - Move around cycle $\eta$ times in all to adjust phase
  - $t_1 = t_2 + c\eta \mod r$
  - Also called $\lambda\rho$ collision or $\rho'$ collision
  - Needs 2 $f$-collisions
Collision Probabilities on $f^r$
Collision Probabilities on $f^r$

- **Rho collision:**
Collision Probabilities on $f^r$

- **Rho collision:**
  - $q$-query feedback attack from some point $x$
Collision Probabilities on $f^r$

- **Rho collision:**
  - $q$-query feedback attack from some point $x$
  - Collision probability $c_{p,\rho}[q]$
Collision Probabilities on $f^r$

- **Rho collision:**
  - $q$-query feedback attack from some point $x$
  - Collision probability $c_{p\rho}[q]$
  
  \[
  c_{p\rho}[q] = O\left(\frac{q^2r}{N}\right)
  \]
Collision Probabilities on $f^r$

- **Rho collision:**
  - $q$-query feedback attack from some point $x$
  - collision probability $cp_\rho[q]

\[
   cp_\rho[q] = O\left(\frac{q^2r}{N}\right)
\]

- **Lambda collision:**
Collision Probabilities on $f^r$

- **Rho collision:**
  - $q$-query feedback attack from some point $x$
  - Collision probability $cp_{\rho}[q]$
    
    $cp_{\rho}[q] = O\left(\frac{q^2r}{N}\right)$

- **Lambda collision:**
  - $(q_1, q_2)$-query two-trail attack from some points $x_1, x_2$
Collision Probabilities on $f^r$

- **Rho collision:**
  - $q$-query feedback attack from some point $x$
  - Collision probability $\text{cp}_\rho[q]$
    \[
    \text{cp}_\rho[q] = O\left(\frac{q^2 r}{N}\right)
    \]

- **Lambda collision:**
  - $(q_1, q_2)$-query two-trail attack from some points $x_1, x_2$
  - Collision probability $\text{cp}_\lambda[q_1, q_2]$
Collision Probabilities on $f^r$

- **Rho collision:**
  - $q$-query feedback attack from some point $x$
  - Collision probability $cp_\rho[q]$
    $$cp_\rho[q] = O\left(\frac{q^2r}{N}\right)$$

- **Lambda collision:**
  - $(q_1, q_2)$-query two-trail attack from some points $x_1, x_2$
  - Collision probability $cp_\lambda[q_1, q_2]$
    $$cp_\lambda[q_1, q_2] = O\left(\frac{q_1q_2r(\log r)^3}{N}\right)$$
Collision Probabilities on $f^r$

A general attack strategy, covering all adversaries:
Collision Probabilities on $f^r$

A general attack strategy, covering all adversaries:

- $m$ trails from $m$ distinct starting points $x_1, \ldots, x_m$
Collision Probabilities on $f^r$

A general attack strategy, covering all adversaries:

- $m$ trails from $m$ distinct starting points $x_1, \ldots, x_m$
- Trail lengths $q_1, \ldots, q_m$ with $\sum_i q_i = q$
Collision Probabilities on $f^r$

A general attack strategy, covering all adversaries:

- $m$ trails from $m$ distinct starting points $x_1, \ldots, x_m$
- Trail lengths $q_1, \ldots, q_m$ with $\sum_i q_i = q$
- Tries to find either a $\rho$ collision or a two-trail $\lambda$ collision

Collision probability $c_p[q]$
Collision Probabilities on $f^r$

A general attack strategy, covering all adversaries:

- $m$ trails from $m$ distinct starting points $x_1, \ldots, x_m$
- Trail lengths $q_1, \ldots, q_m$ with $\sum_i q_i = q$
- Tries to find either a $\rho$ collision or a two-trail $\lambda$ collision
- Collision probability $cp[q]$
Collision Probabilities on $f^r$

A general attack strategy, covering all adversaries:

- $m$ trails from $m$ distinct starting points $x_1, \ldots, x_m$
- Trail lengths $q_1, \ldots, q_m$ with $\sum_i q_i = q$
- Tries to find either a $\rho$ collision or a two-trail $\lambda$ collision
- Collision probability $cp[q]$

$$cp[q] = O\left(\frac{q^2 r (\log r)^3}{N}\right)$$
PRF Security Result

A any prf adversary $\text{Adv}_{\text{prf}}$ $f$ = $O(q^2 r (\log r)^3 N)$

Proof uses Patarin's Coefficient H Technique

$(\log r)^3$ can be further improved, almost to $\log r$

Probably possible to show $\text{Adv}_{\text{prf}}$ $f$ = $O(q^2 r N)$
PRF Security Result

- $A$ any prf adversary
PRF Security Result

- $A$ any prf adversary

$$\text{Adv}_A^{prf} [f^r] = O \left( \frac{q^2 r (\log r)^3}{N} \right)$$
PRF Security Result

- \( \mathcal{A} \) any prf adversary

- \[
\text{Adv}^\text{prf}_\mathcal{A} [f^r] = O \left( \frac{q^2 r (\log r)^3}{N} \right)
\]

- Proof uses Patarin’s Coefficient H Technique
PRF Security Result

- $\mathcal{A}$ any prf adversary

$$\text{Adv}^\text{prf}_\mathcal{A}[f^r] = O\left(\frac{q^2 r (\log r)^3}{N}\right)$$

- Proof uses *Patarin’s Coefficient H Technique*

- $(\log r)^3$ can be further improved, almost to $\log r$
PRF Security Result

- $A$ any prf adversary

\[ \text{Adv}^{\text{prf}}_{A} [f^r] = O \left( \frac{q^2 r (\log r)^3}{N} \right) \]

- Proof uses Patarin’s Coefficient H Technique

- $(\log r)^3$ can be further improved, almost to $\log r$

- Probably possible to show $\text{Adv}^{\text{prf}}_{A} [f^r] = O \left( \frac{q^2 r}{N} \right)$
Iterated Random Function

Sketch of Proof

Parallel Graph: union of non-intersecting paths

Query transcript $\tau$ has multiple trails

Call $\tau$ BAD if not parallel graph

BAD is equivalent to collision in general $m$ trail attack (after reordering queries)

$$\Pr[\text{BAD}] = O\left(q^2 r (\log r)^3 N\right)$$

Internal states equally probable for isomorphic good transcripts

Plug internal blocks into the good transcript $\tau$
Sketch of Proof

- **Parallel Graph**: union of non-intersecting paths
Sketch of Proof

- **Parallel Graph**: union of non-intersecting paths
- Query transcript $\tau$ has multiple trails
**Sketch of Proof**

- **Parallel Graph**: union of non-intersecting paths
- Query transcript $\tau$ has multiple trails
- Call $\tau$ BAD if not parallel graph
Sketch of Proof

- **Parallel Graph**: union of non-intersecting paths
- Query transcript $\tau$ has multiple trails
- Call $\tau$ BAD if not parallel graph
- BAD is equivalent to collision in general $m$ trail attack (after reordering queries)
Sketch of Proof

- **Parallel Graph**: union of non-intersecting paths
- Query transcript $\tau$ has multiple trails
- Call $\tau$ BAD if not parallel graph
- BAD is equivalent to collision in general $m$ trail attack (after reordering queries)

$$\Pr[\text{BAD}] = O\left(\frac{q^2 r (\log r)^3}{N}\right)$$
Parallel Graph: union of non-intersecting paths

Query transcript $\tau$ has multiple trails

Call $\tau$ BAD if not parallel graph

BAD is equivalent to collision in general $m$ trail attack (after reordering queries)

\[
\Pr [BAD] = O \left( \frac{q^2 r (\log r)^3}{N} \right)
\]

Internal states equally probable for isomorph ic good transcripts
Sketch of Proof

- **Parallel Graph**: union of non-intersecting paths
- Query transcript $\tau$ has multiple trails
- Call $\tau$ BAD if not parallel graph
- BAD is equivalent to collision in general $m$ trail attack (after reordering queries)

\[
\Pr [BAD] = O \left( \frac{q^2 r (\log r)^3}{N} \right)
\]

- Internal states equally probable for isomorphic good transcripts
- Plug internal blocks into the good transcript $\tau$
Lower Bound on Collision Probability
Lower Bound on Collision Probability

- General $m$ trail attack is the best known attack
General $m$ trail attack is the best known attack

$cp[q]$ is best known success probability
Lower Bound on Collision Probability

- General $m$ trail attack is the best known attack
- $cp[q]$ is best known success probability
- Inclusion-Exclusion Principle gives lower bound
Lower Bound on Collision Probability

- General $m$ trail attack is the best known attack
- $cp[q]$ is best known success probability
- Inclusion-Exclusion Principle gives lower bound

$$cp[q] = \Omega \left( \frac{q^2 r}{N} \right)$$
General $m$ trail attack is the best known attack

cp[$q$] is best known success probability

Inclusion-Exclusion Principle gives lower bound

$$\text{cp}[q] = \Omega \left( \frac{q^2 r}{N} \right)$$

Security bound tight up to a factor of $(\log r)^3$
Lower Bound on Collision Probability

\[ x := (x_1, x_2, \ldots, x_q), \text{ } x_i \text{ are distinct blocks from } \{0, 1\}^n. \]

Let \( \text{coll}_f(x_i; x_j) \) denote the event \( f^{(\ell)}(x_i) = f^{(\ell)}(x_j) \) and 
\( \text{coll}_f(x) := \bigcup_{x_i, x_j \in x} \text{coll}_f(x_i; x_j). \)
Lower Bound on Collision Probability

\[
\Pr_f[\text{coll}_f(x)] \geq \sum_{i<j} \Pr_f[\text{coll}_f(x_i; x_j)] - 3 \sum_{i<j<k} \Pr_f[\text{coll}_f(x_i; x_j) \cap \text{coll}_f(x_j; x_k)] - \frac{1}{2} \sum_{i<j,k<m \{i,j\} \cap \{k,m\} = 0} \Pr_f[\text{coll}_f(x_i; x_j) \cap \text{coll}_f(x_k; x_m)]
\]
Upper Bound on $\text{coll}_{i,j,k}$

$$\Pr[\text{Case 1}] \leq \frac{2\ell^2}{N^2}$$

$$\Pr[\text{Case 2}] \leq \frac{6\ell^6}{N^3}$$

$$\text{coll}_{i,j,k} \leq \frac{2\ell^2}{N^2} + \frac{6\ell^6}{N^3}.$$
Upper Bound on $\text{coll}_{i,j,k,m}$

- Pr[Case 1] $\leq \frac{\ell^2}{N^2}$
- Pr[Case 2] $\leq \frac{6\ell^3}{N^3}$
- Pr[Case 3] $\leq \frac{2\ell^5}{N^3}$
Upper Bound on $\text{coll}_{i,j,k,m}$

Pr[Case 4] $\leq \frac{24\ell^8}{N^4}$

Pr[Case 5] $\leq \frac{4\ell^8}{N^4}$.

$\text{coll}_{i,j,k,m} \leq \frac{\ell^2}{N^2} + \frac{6\ell^3 + 2\ell^5}{N^3} + \frac{28\ell^8}{N^4}$. 

Let $\text{cycle}$ be the event that at least one of the walks (corresponding to $x_i$ and $x_j$) has a cycle.

\[
\text{coll}_{i,j} \mid \lnot \text{cycle} = \frac{\ell}{N} \quad \text{Pr}[\text{cycle}] \leq \frac{2\ell^2}{N}.
\]

\[
\text{coll}_{i,j} \geq \frac{\ell}{N} \left(1 - \frac{2\ell^2}{N}\right).
\]
Main Result on Lower Bound

**Lower Bound Theorem**

Let \( x := (x_1, \ldots, x_q) \in (\{0, 1\}^n)^q \) be a \( q \) tuple of distinct inputs.
For \( \ell, q \geq 3, \frac{q^2 \ell}{N} < 1 \) and \( \ell < \min\left( \frac{N}{5184}, \frac{N^{\frac{1}{2}}}{4\sqrt{3}}, \frac{N^{\frac{1}{3}}}{3\sqrt{36}} \right) \), we have

\[
\Pr[\text{coll}_f(x)] \geq \frac{q^2 \ell}{12N}.
\]

**Example**

Collision for \( N = 2^{64} \). Hence taking \( q = \sqrt{20} \cdot 2^{\frac{64}{3}}, \ell = 0.1 \times 2^{\frac{64}{3}} \), we get \( \delta = 0.499 \).
Future Research and Conclusion

- Removing log \( r \) factor.
Future Research and Conclusion

- Removing log $r$ factor.
- The attack requires some lower bound on $q$. Can we prove some lower bound for all attacks?
Future Research and Conclusion

- Removing log $r$ factor.
- The attack requires some lower bound on $q$. Can we prove some lower bound for all attacks?
- Almost tight bound (up to a log $r$ factor).
Future Research and Conclusion

- Removing log $r$ factor.
- The attack requires some lower bound on $q$. Can we prove some lower bound for all attacks?

- Almost tight bound (up to a log $r$ factor).

THANK YOU
Conclusion