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.

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 Probabilties and PRF analysis

The Iterated Random Permutations Problem

The Iterated Random Permutations Problem

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

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 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 $\Theta(rq^2/2^n)$ PRF advantage
- We show an attack with advantage about $rq^2/2^n$ 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

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**:

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: $\boxed{x}$, query i: $\boxed{f^{i-1}(x)}$

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: $\boxed{x}$, query i: $\boxed{f^{i-1}(x)}$
  - 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: $\boxed{x}$, query i: $\boxed{f^{i-1}(x)}$
  - 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: $\boxed{x}$, query i: $\boxed{f^{i-1}(x)}$
  - 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: $\boxed{x}$, query i: $\boxed{f^{i-1}(x)}$
  - 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: $\boxed{x}$, query i: $\boxed{f^{i-1}(x)}$
  - 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: $\boxed{x_j}$, query i on Trail j: $\boxed{f^{i-1}(x_j)}$

Collision Attack on f

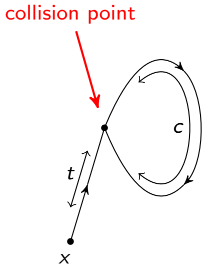
Two main approaches:

- **Feedback Attack**:
  - Based on Pollard's Rho Algorithm
  - Keeps feeding back f's outputs to f
  - Query 1: $\boxed{x}$, query i: $\boxed{f^{i-1}(x)}$
  - 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: $\boxed{x_j}$, query i on Trail j: $\boxed{f^{i-1}(x_j)}$
  - Tries to make two trails merge

Collision Types on f

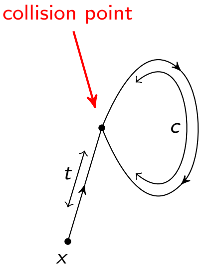
Collision Types on f

- **Rho collision**



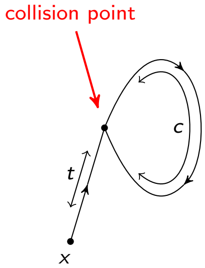
Collision Types on f

- **Rho collision**
  - Tail length t



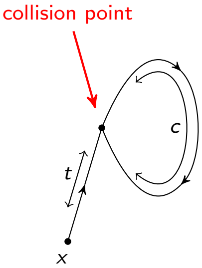
Collision Types on f

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



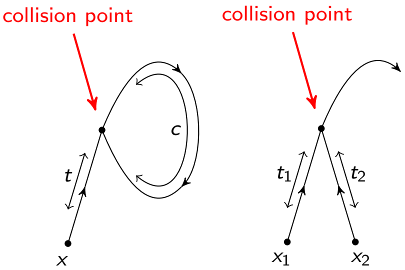
Collision Types on f

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



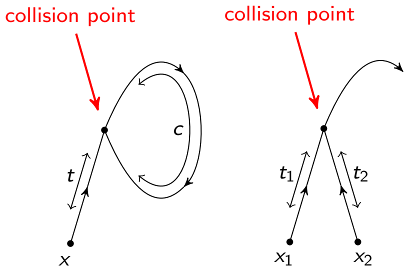
Collision Types on f

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



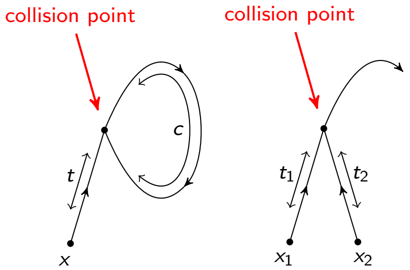
Collision Types on f

- **Rho collision**
  - Tail length t
  - Cycle length c
  - Denoted $\rho(t, c)$
- **Lambda collision**
  - Foot lengths t_1 and t_2

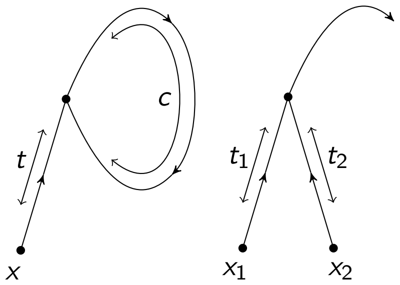


Collision Types on f

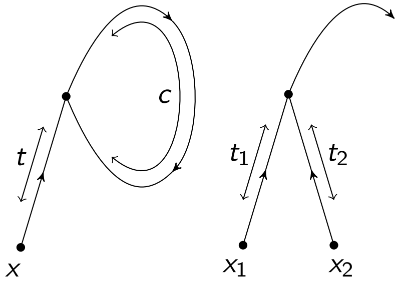
- **Rho collision**
  - Tail length t
  - Cycle length c
  - Denoted $\rho(t, c)$
- **Lambda collision**
  - Foot lengths t_1 and t_2
  - Denoted $\lambda(t_1, t_2)$



Collision Probabilities on f

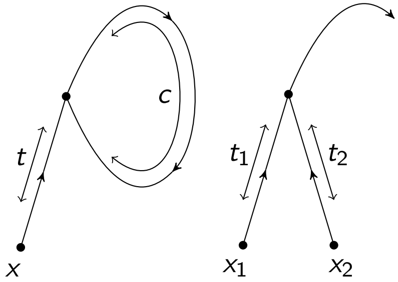


Collision Probabilities on f



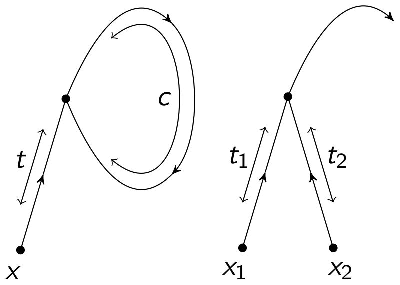
- **Rho collision**

Collision Probabilities on f



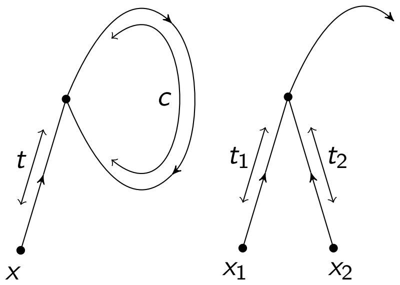
- **Rho collision**
  - Feedback attack from some x

Collision Probabilities on f



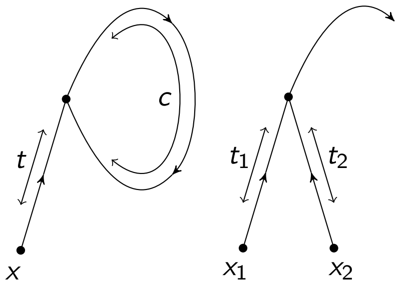
- **Rho collision**
  - Feedback attack from some x
  - $\Pr\left[\rho(t, c)\right] \leq \frac{1}{N}$

Collision Probabilities on f



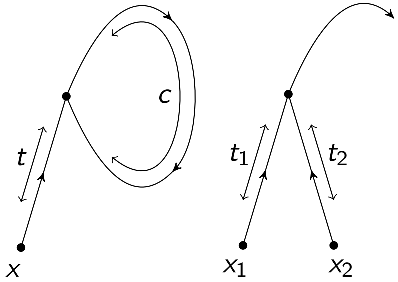
- **Rho collision**
  - Feedback attack from some x
  - $\Pr\left[\rho(t,c)\right] \leq \frac{1}{N}$
  - $\Pr\left[\rho(t,c)\right] \leq \frac{e^{-\alpha}}{N}$ for $t = \Theta(\sqrt{\alpha N})$

Collision Probabilities on f



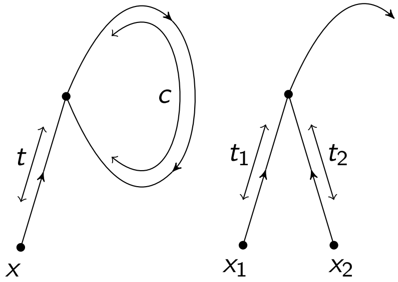
- **Rho collision**
  - Feedback attack from some x
  - $\Pr\left[\rho(t,c)\right] \leq \frac{1}{N}$
  - $\Pr\left[\rho(t,c)\right] \leq \frac{e^{-\alpha}}{N}$ for $t = \Theta(\sqrt{\alpha N})$
- **Lambda collision**

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
  - $\Pr\left[\rho(t, c)\right] \leq \frac{1}{N}$
  - $\Pr\left[\rho(t, c)\right] \leq \frac{e^{-\alpha}}{N}$ for $t = \Theta(\sqrt{\alpha N})$
- **Lambda collision**
  - Two-trail attack from some x_1 and x_2
  - $\Pr\left[\lambda(t_1, t_2)\right] \leq \frac{1}{N}$

Collision Attack on f^r

Same two approaches:

Collision Attack on f^r

Same two approaches:

- **Feedback Attack**:

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: $\boxed{x}$, query i: $\boxed{(f^r)^{i-1}(x)}$

Collision Attack on f^r

Same two approaches:

- **Feedback Attack**:
  - Keeps feeding back f^r's outputs to f^r
  - Query 1: $\boxed{x}$, query i: $\boxed{(f^r)^{i-1}(x)}$
  - 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: $\boxed{x}$, query i: $\boxed{(f^r)^{i-1}(x)}$
  - 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: $\boxed{x}$, query i: $\boxed{(f^r)^{i-1}(x)}$
  - 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: $\boxed{x}$, query i: $\boxed{(f^r)^{i-1}(x)}$
  - Tries to find cycle
- **Multiple Trails Attack**:
  - Starts feedback queries simultaneously from many points
  - Query 1 on Trail j: $\boxed{x_j}$, query i on Trail j: $\boxed{(f^r)^{i-1}(x_j)}$

Collision Attack on f^r

Same two approaches:

- **Feedback Attack**:
  - Keeps feeding back f^r's outputs to f^r
  - Query 1: $\boxed{x}$, query i: $\boxed{(f^r)^{i-1}(x)}$
  - Tries to find cycle
- **Multiple Trails Attack**:
  - Starts feedback queries simultaneously from many points
  - Query 1 on Trail j: $\boxed{x_j}$, query i on Trail j: $\boxed{(f^r)^{i-1}(x_j)}$
  - Tries to make two trails merge

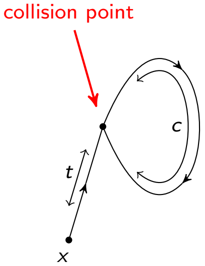
Collision Types on f^r

Collision Types on f^r

- Can be reduced to collisions on f

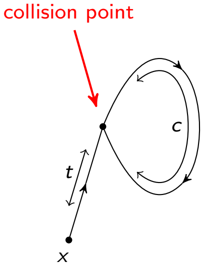
Collision Types on f^r

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



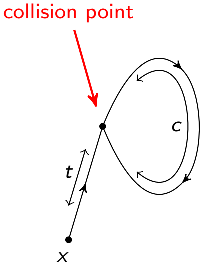
Collision Types on f^r

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



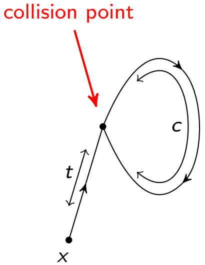
Collision Types on f^r

- Can be reduced to collisions on f
- **Rho collision:**
  - *Direct ρ collision:*
    - f-collision in phase with r



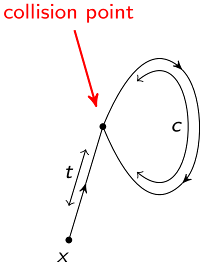
Collision Types on f^r

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



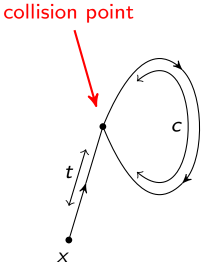
Collision Types on f^r

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



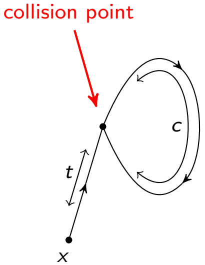
Collision Types on f^r

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



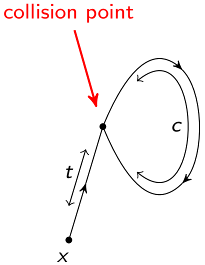
Collision Types on f^r

- Can be reduced to collisions on f
- **Rho collision:**
  - *Direct ρ collision:*
    - f-collision in phase with r
    - $t = t + c \bmod r$
  - *Delayed ρ collision:*
    - f-collision out of phase
    - move around cycle η times in all to adjust phase



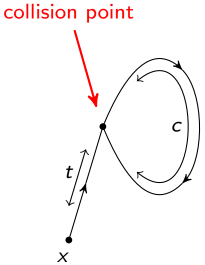
Collision Types on f^r

- Can be reduced to collisions on f
- **Rho collision:**
  - *Direct ρ collision:*
    - f-collision in phase with r
    - $t = t + c \bmod r$
  - *Delayed ρ collision:*
    - f-collision out of phase
    - move around cycle η times in all to adjust phase
    - $\eta = r/\gcd(c, r)$



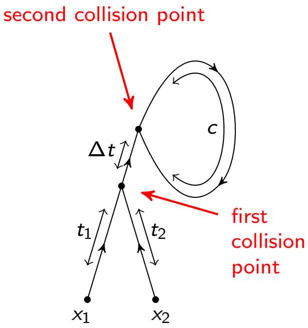
Collision Types on f^r

- Can be reduced to collisions on f
- **Rho collision:**
  - *Direct ρ collision:*
    - f-collision in phase with r
    - $t = t + c \bmod r$
  - *Delayed ρ collision:*
    - f-collision out of phase
    - move around cycle η times in all to adjust phase
    - $\eta = r/\gcd(c, r)$
    - $t = t + c\eta \bmod r$



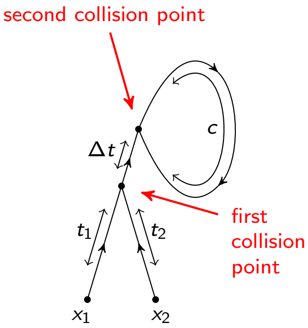
Collision Types on f^r

- Can be reduced to collisions on f
- **Lambda collision:**



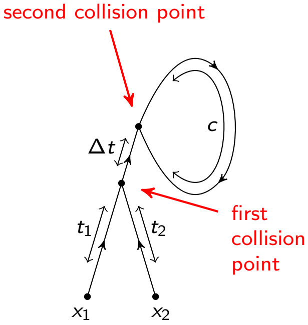
Collision Types on f^r

- Can be reduced to collisions on f
- **Lambda collision:**
  - *Direct λ collision:*



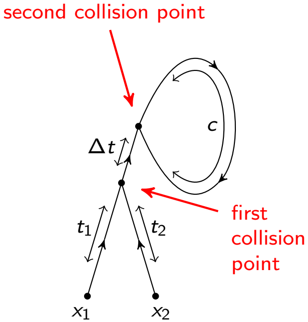
Collision Types on f^r

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



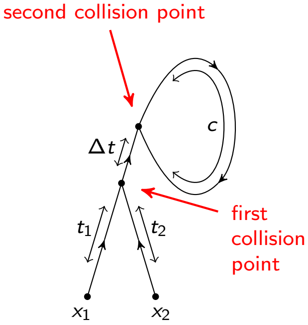
Collision Types on f^r

- Can be reduced to collisions on f
- **Lambda collision:**
    - *Direct λ collision:*
        - f-collision in phase with r
        - $t_1 = t_2 \bmod r$



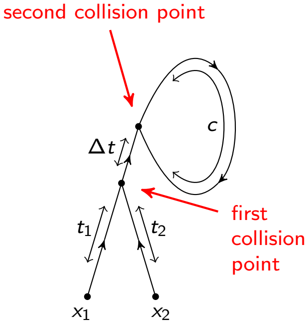
Collision Types on f^r

- Can be reduced to collisions on f
- **Lambda collision:**
  - *Direct λ collision:*
    - f-collision in phase with r
    - $t_1 = t_2 \bmod r$
  - *Delayed λ collision:*



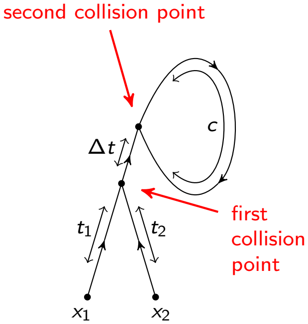
Collision Types on f^r

- Can be reduced to collisions on f
- **Lambda collision:**
  - *Direct λ collision:*
    - f-collision in phase with r
    - $t_1 = t_2 \bmod r$
  - *Delayed λ collision:*
    - f-collision out of phase



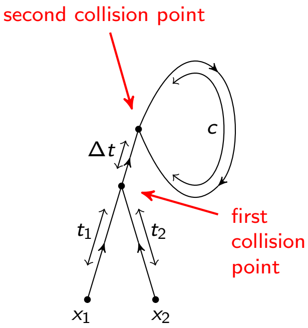
Collision Types on f^r

- Can be reduced to collisions on f
- **Lambda collision:**
  - *Direct λ collision:*
    - f-collision in phase with r
    - $t_1 = t_2 \bmod r$
  - *Delayed λ collision:*
    - f-collision out of phase
    - find ρ collision on merged walk



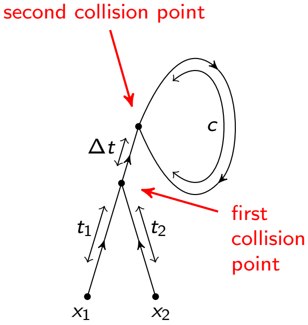
Collision Types on f^r

- Can be reduced to collisions on f
- **Lambda collision:**
  - *Direct λ collision:*
    - f-collision in phase with r
    - $t_1 = t_2 \bmod r$
  - *Delayed λ collision:*
    - f-collision out of phase
    - find ρ collision on merged walk
    - move around cycle η times in all to adjust phase



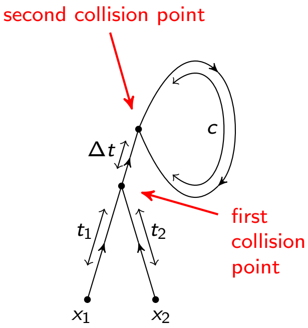
Collision Types on f^r

- Can be reduced to collisions on f
- **Lambda collision:**
  - *Direct λ collision:*
    - f-collision in phase with r
    - $t_1 = t_2 \bmod r$
  - *Delayed λ collision:*
    - f-collision out of phase
    - find ρ collision on merged walk
    - move around cycle η times in all to adjust phase
    - $t_1 = t_2 + c\eta \bmod r$



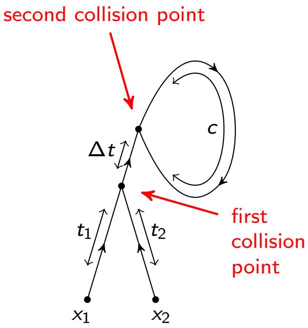
Collision Types on f^r

- Can be reduced to collisions on f
- **Lambda collision:**
  - *Direct λ collision:*
    - f-collision in phase with r
    - $t_1 = t_2 \mod r$
  - *Delayed λ collision:*
    - f-collision out of phase
    - find ρ collision on merged walk
    - move around cycle η times in all to adjust phase
    - $t_1 = t_2 + c\eta \mod r$
    - also called $\lambda\rho$ collision or ρ' collision



Collision Types on f^r

- Can be reduced to collisions on f
- **Lambda collision:**
  - *Direct λ collision:*
    - f-collision in phase with r
    - $t_1 = t_2 \bmod r$
  - *Delayed λ collision:*
    - f-collision out of phase
    - find ρ collision on merged walk
    - move around cycle η times in all to adjust phase
    - $t_1 = t_2 + c\eta \bmod r$
    - also called $\lambda\rho$ collision or ρ' 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 $\mathrm{cp}_\rho[q]$

Collision Probabilities on f^r

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

Collision Probabilities on f^r

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

Collision Probabilities on f^r

- **Rho collision:**
  - q-query feedback attack from some point x
  - collision probability $\mathrm{cp}_\rho[q]$
  - $\boxed{\mathrm{cp}_\rho[q] = O\left(\frac{q^2 r}{N}\right)}$
- **Lambda collision:**
  - (q_1, q_2)-query two-trail attack from some points x_1, x_2

Collision Probabilities on f^r

- **Rho collision:**
  - q-query feedback attack from some point x
  - collision probability $\mathrm{cp}_\rho[q]$
  - $\boxed{\mathrm{cp}_\rho[q] = O\left(\frac{q^2 r}{N}\right)}$
- **Lambda collision:**
  - (q_1, q_2)-query two-trail attack from some points x_1, x_2
  - collision probability $\mathrm{cp}_\lambda[q_1, q_2]$

Collision Probabilities on f^r

- **Rho collision:**
  - q-query feedback attack from some point x
  - collision probability $\mathrm{cp}_\rho[q]$
  - $\boxed{\mathrm{cp}_\rho[q] = O\left(\frac{q^2 r}{N}\right)}$
- **Lambda collision:**
  - (q_1, q_2)-query two-trail attack from some points x_1, x_2
  - collision probability $\mathrm{cp}_\lambda[q_1, q_2]$
  - $\boxed{\mathrm{cp}_\lambda[q_1, q_2] = O\left(\frac{q_1 q_2 r (\log r)^3}{N}\right)}$

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 ρ collision or a two-trail λ collision

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 ρ collision or a two-trail λ collision
- Collision probability $\mathrm{cp}[q]$

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 ρ collision or a two-trail λ collision
- Collision probability $\mathrm{cp}[q]$
- $\boxed{\mathrm{cp}[q] = O\left(\frac{q^2 r (\log r)^3}{N}\right)}$

PRF Security Result

PRF Security Result

- $\mathcal{A}$ any prf adversary

PRF Security Result

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

PRF Security Result

- $\mathcal{A}$ any prf adversary
- $\boxed{\mathbf{Adv}^{prf}_{\mathcal{A}}[f^r] = O\left(\frac{q^2 r (\log r)^3}{N}\right)}$
- Proof uses *Patarin's Coefficient H Technique*

PRF Security Result

- $\mathcal{A}$ any prf adversary
- $\boxed{\mathbf{Adv}_{\mathcal{A}}^{prf}[f^r] = O\left(\frac{q^2 r (\log r)^3}{N}\right)}$
- Proof uses *Patarin's Coefficient H Technique*
- $(\log r)^3$ can be further improved, almost to $\log r$

PRF Security Result

- $\mathcal{A}$ any prf adversary
- $\boxed{\mathbf{Adv}^{prf}_{\mathcal{A}}[f^r] = O\left(\frac{q^2 r (\log r)^3}{N}\right)}$
- Proof uses *Patarin's Coefficient H Technique*
- $(\log r)^3$ can be further improved, almost to $\log r$
- Probably possible to show $\mathbf{Adv}^{prf}_{\mathcal{A}}[f^r] = O\left(\frac{q^2 r}{N}\right)$

Sketch of Proof

Sketch of Proof

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

Sketch of Proof

- **Parallel Graph**: union of non-intersecting paths
- Query transcript τ has multiple trails

Sketch of Proof

- **Parallel Graph**: union of non-intersecting paths
- Query transcript τ has multiple trails
- Call τ BAD if not parallel graph

Sketch of Proof

- **Parallel Graph**: union of non-intersecting paths
- Query transcript τ has multiple trails
- Call τ 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 τ has multiple trails
- Call τ BAD if not parallel graph
- BAD is equivalent to collision in general m trail attack (after reordering queries)
- $\boxed{\Pr[BAD] = O\left(\frac{q^2 r (\log r)^3}{N}\right)}$

Sketch of Proof

- **Parallel Graph**: union of non-intersecting paths
- Query transcript τ has multiple trails
- Call τ BAD if not parallel graph
- BAD is equivalent to collision in general m trail attack (after reordering queries)
- $\boxed{\Pr[BAD] = O\left(\frac{q^2 r(\log r)^3}{N}\right)}$
- Internal states equally probable for isomorphic good transcripts

Sketch of Proof

- **Parallel Graph**: union of non-intersecting paths
- Query transcript τ has multiple trails
- Call τ BAD if not parallel graph
- BAD is equivalent to collision in general m trail attack (after reordering queries)
- $\boxed{\Pr[BAD] = O\left(\frac{q^2 r(\log r)^3}{N}\right)}$
- Internal states equally probable for isomorphic good transcripts
- Plug internal blocks into the good transcript τ

Lower Bound on Collision Probability

Lower Bound on Collision Probability

- General m trail attack is the best known attack

Lower Bound on Collision Probability

- 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
- $\mathrm{cp}[q]$ 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
- $\mathrm{cp}[q]$ is best known success probability
- Inclusion-Exclusion Principle gives lower bound
- $\boxed{\mathrm{cp}[q] = \Omega\left(\frac{q^2 r}{N}\right)}$

Lower Bound on Collision Probability

- General m trail attack is the best known attack
- $\mathrm{cp}[q]$ is best known success probability
- Inclusion-Exclusion Principle gives lower bound
- $\boxed{\mathrm{cp}[q] = \Omega\left(\frac{q^2 r}{N}\right)}$
- Security bound tight up to a factor of $(\log r)^3$

Lower Bound on Collision Probability

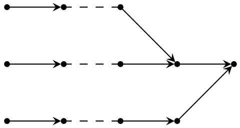
$x := (x_1, x_2, \ldots, x_q)$, x_i are distinct blocks from $\{0,1\}^n$.

Let $\mathbf{coll}_f(x_i; x_j)$ denote the event $f^{(\ell)}(x_i) = f^{(\ell)}(x_j)$ and $\mathbf{coll}_f(x) := \bigcup_{x_i, x_j \in x} \mathbf{coll}_f(x_i; x_j)$.

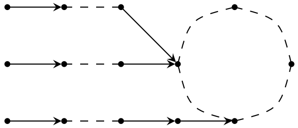
Lower Bound on Collision Probability

$$
\begin{aligned}
\Pr_f\left[\mathbf{coll}_f(x)\right] \geq{} & \sum_{i<j} \overbrace{\Pr_f[\mathbf{coll}_f(x_i; x_j)]}^{\mathbf{coll}_{i,j}} \\
& - 3 \sum_{i<j<k} \overbrace{\Pr_f[\mathbf{coll}_f(x_i; x_j) \cap \mathbf{coll}_f(x_j; x_k)]}^{\mathbf{coll}_{i,j,k}} \\
& - \frac{1}{2} \sum_{\substack{i<j, k<m \\ \{i,j\}\cap\{k,m\}=\emptyset}} \overbrace{\Pr_f[\mathbf{coll}_f(x_i; x_j) \cap \mathbf{coll}_f(x_k; x_m)]}^{\mathbf{coll}_{i,j,k,m}}
\end{aligned}
$$

Upper Bound on $\mathbf{coll}_{i,j,k}$



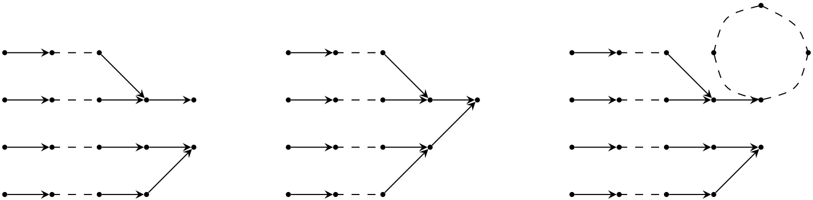
$\Pr[\text{Case 1}] \leq \frac{2\ell^2}{N^2}$



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

$$\boxed{\mathbf{coll}_{i,j,k} \leq \frac{2\ell^2}{N^2} + \frac{6\ell^6}{N^3}.}$$

Upper Bound on $\mathbf{coll}_{i,j,k,m}$

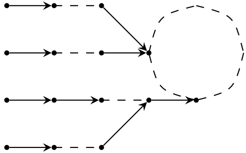


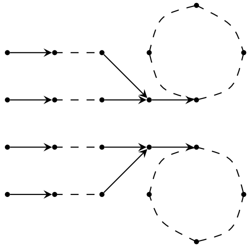
$\Pr[\texttt{Case 1}] \leq \frac{\ell^2}{N^2}$

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

$\Pr[\texttt{Case 3}] \leq \frac{2\ell^5}{N^3}$

Upper Bound on $\mathbf{coll}_{i,j,k,m}$





$$\Pr[\text{Case } 4] \leq \frac{24\ell^8}{N^4} \qquad \Pr[\text{Case } 5] \leq \frac{4\ell^8}{N^4}.$$

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

Lower Bound on $\mathbf{coll}_{i,j}$

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

$$\mathbf{coll}_{i,j|\neg\texttt{cycle}} = \frac{\ell}{N} \qquad \Pr[\texttt{cycle}] \leq \frac{2\ell^2}{N}.$$

$$\boxed{\mathbf{coll}_{i,j} \geq \frac{\ell}{N}\left(1 - \frac{2\ell^2}{N}\right).}$$

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 $\ell < \min(\frac{N}{5184}, \frac{N^{\frac{1}{2}}}{4\sqrt{3}}, \frac{N^{\frac{1}{3}}}{\sqrt[3]{36}})$, we have

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

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 $\delta = 0.499$. $\square$

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