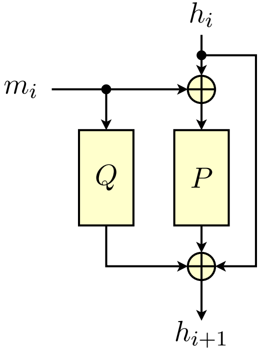
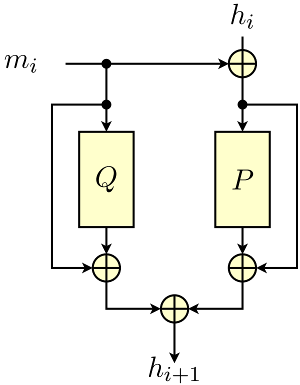
$$h_{i+1} = f(h_i, m_i) = h_i \oplus P(h_i \oplus m_i) \oplus Q(m_i)$$

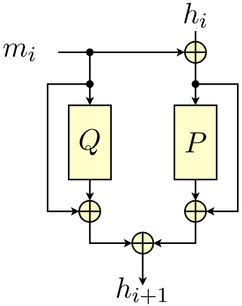
Standard description

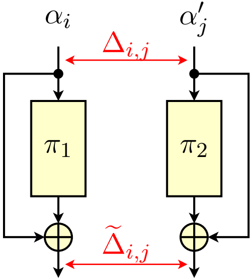


Alternative description



The graph construction





Queries

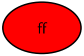
- to π_1: $R_1 = \{\alpha_i : 1 \leq i \leq q_1\}$
- to π_2: $R_2 = \{\alpha'_j : 1 \leq j \leq q_2\}$

The graph

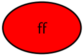
- Nodes: $\mathsf{V} = \{IV\} \cup \{\Delta_{i,j}, \widetilde{\Delta}_{i,j} : 1 \leq i \leq q_1, 1 \leq j \leq q_2\}$
- Edges: $\mathsf{E} = \{(\Delta_{i,j}, \widetilde{\Delta}_{i,j}; \alpha_i) : 1 \leq i \leq q_1, 1 \leq j \leq q_2\}$

Correspondence

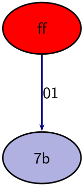
- $\alpha_i \longleftrightarrow m_i$ (message blocks)
- $\Delta, \widetilde{\Delta} \longleftrightarrow h$ (chaining values)
- Labeling of paths rooted in $IV \longleftrightarrow$ messages we can hash without new queries



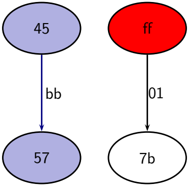
$R_1 = \{\}$
$R_2 = \{\}$



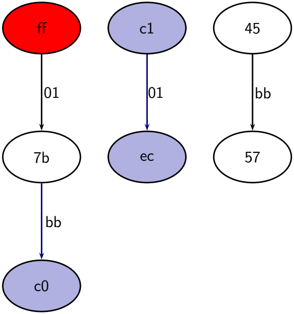
$R_1 = \{\texttt{0x01}\}$
$R_2 = \{\}$



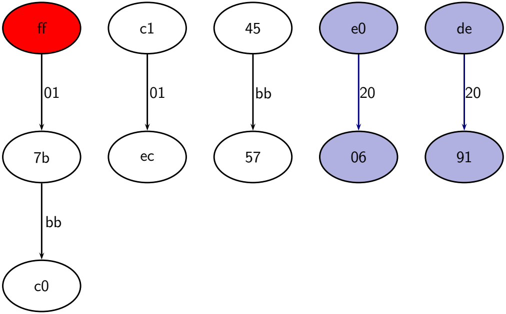
$R_1 = \{\texttt{0x01}\}$
$R_2 = \{\texttt{0xfe}\}$



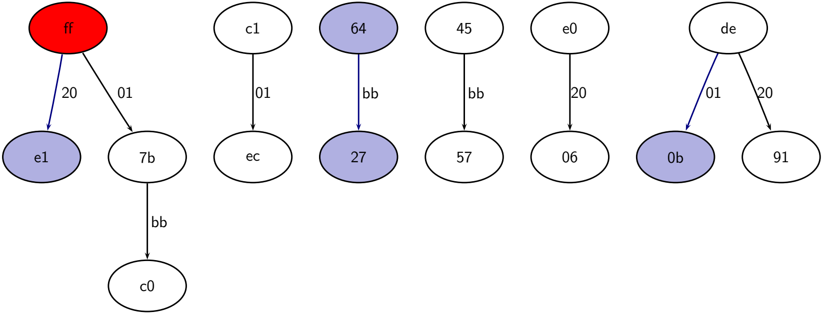
$R_1 = \{\texttt{0x01}, \texttt{0xbb}\}$
$R_2 = \{\texttt{0xfe}\}$



$$R_1 = \{\mathtt{0x01}, \mathtt{0xbb}\}$$
$$R_2 = \{\mathtt{0xfe}, \mathtt{0xc0}\}$$



$R_1 = \{\texttt{0x01}, \texttt{0xbb}, \texttt{0x20}\}$
$R_2 = \{\texttt{0xfe}, \texttt{0xc0}\}$



$$R_1 = \{\texttt{0x01}, \texttt{0xbb}, \texttt{0x20}\}$$
$$R_2 = \{\texttt{0xfe}, \texttt{0xc0}, \texttt{0xdf}\}$$

The security proof

Collision – two distinct paths starting from IV and ending in the same node Δ

Proof outline

- Assume after $q_1 + q_2$ queries we have a graph G
- Do one more query $\tilde{\alpha}$ to π_1 to get $\tilde{\beta} = \pi_1(\tilde{\alpha})$
- Expand the graph to $\tilde{G}$
- Bound the probability of a collision appearing in $\tilde{G}$ provided that there was no collision in G

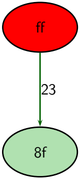
Colliding paths

$$P = \{p \neq \emptyset : \exists \Delta \in V : IV \overset{p}{\rightsquigarrow} \Delta\}$$

Set of all non-empty paths starting from IV
Colliding paths (path is a sequence of edges):

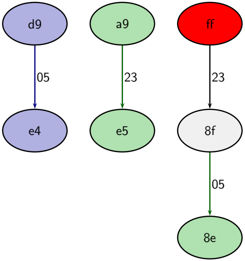
- Path 1: $p \rightarrowtail (IV, \Delta_1, \ldots, \Delta_l = \Delta)$, shorthand: $IV \overset{p}{\rightsquigarrow} \Delta$
- Path 2: $p' \rightarrowtail (IV, \Delta'_1, \ldots, \Delta'_m = \Delta)$, shorthand: $IV \overset{p'}{\rightsquigarrow} \Delta$
- Since there is no collision in G, at least one path must contain vertices from $\tilde{P} \setminus P$
  [in the original paper: "either p or p'"]
- say p is that path

Example



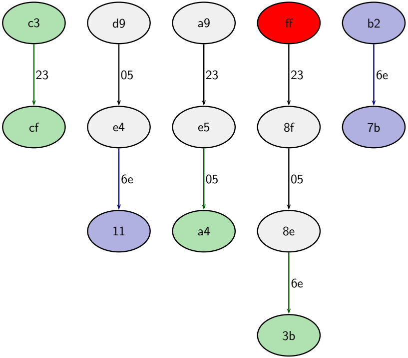
$R1 = \{0x23\}$
$R2 = \{0xdc\}$

Example



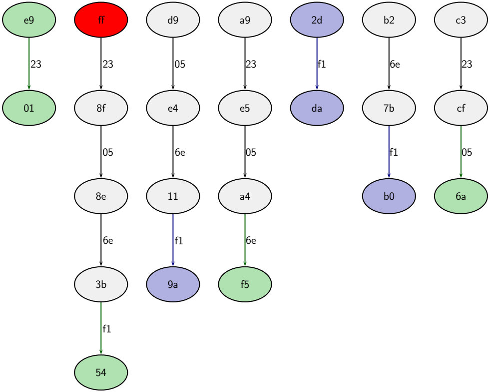
$R1 = \{0x23, 0x05\}$
$R2 = \{0xdc, 0x8a\}$

Example



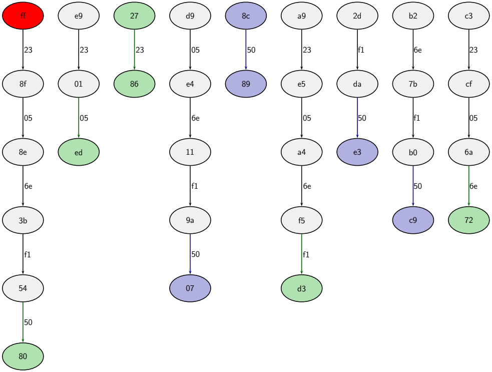
$$R1 = \{0x23, 0x05, 0x6e\}$$
$$R2 = \{0xdc, 0x8a, 0xe0\}$$

Example

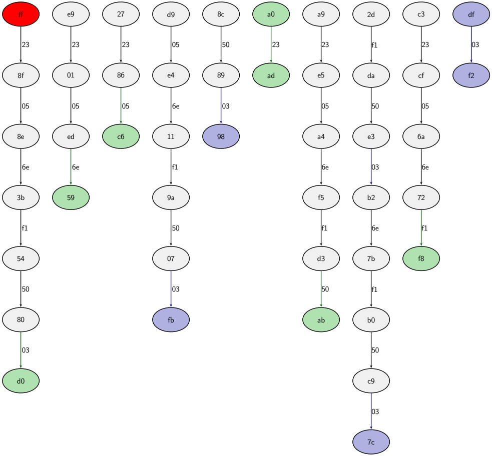


$R1 = \{0x23, 0x05, 0x6e, 0xf1\}$
$R2 = \{0xdc, 0x8a, 0xe0, 0xca\}$

Example

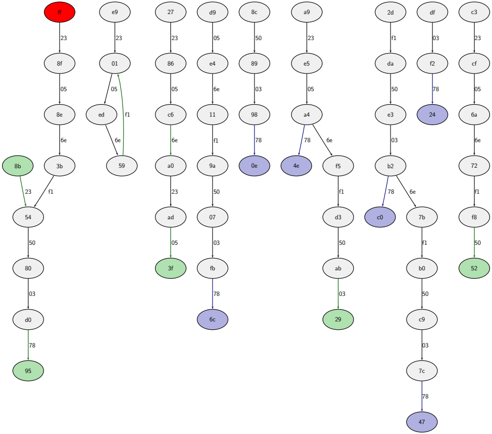


$$R1 = \{0x23, 0x05, 0x6e, 0xf1, 0x50\}$$
$$R2 = \{0xdc, 0x8a, 0xe0, 0xca, 0x04\}$$

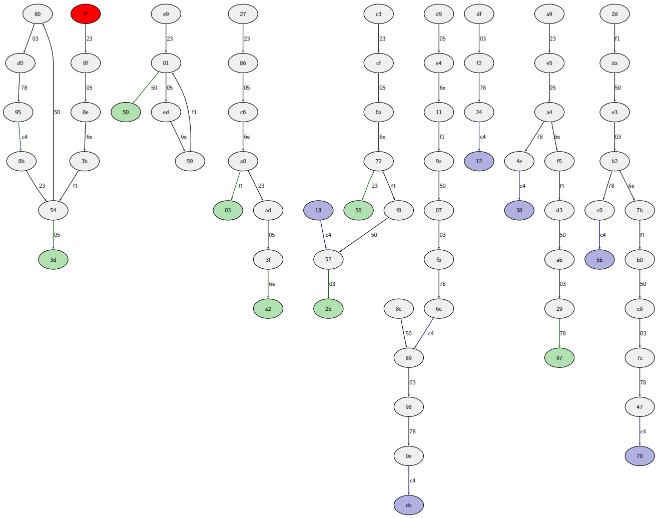


$$R1 = \{0x23, 0x05, 0x6e, 0xf1, 0x50, 0x03\}$$
$$R2 = \{0xdc, 0x8a, 0xe0, 0xca, 0x04\}$$

Example



$$R1 = \{0x23, 0x05, 0x6e, 0xf1, 0x50, 0x03, 0x78\}$$
$$R2 = \{0xdc, 0x8a, 0xe0, 0xca, 0x04, 0x83, 0xa8\}$$



$$R1 = \{0x23, 0x05, 0x6e, 0xf1, 0x50, 0x03, 0x78, 0xc4\}$$
$$R2 = \{0xdc, 0x8a, 0xe0, 0xca, 0x04, 0x83, 0xa8, 0x51\}$$

Three important sets

$$T = \{\Delta \in V : \text{there exists a path from } IV \text{ to } \Delta\}$$
$$A = \{\Delta \oplus \alpha' : \Delta \in T, \alpha' \in R_2\}$$
$$B = \{\alpha' \oplus \pi_2(\alpha') \oplus \Delta : \Delta \in V, \alpha' \in R_2\}$$

- T – set of vertices Δ reachable from IV – corresponds to chaining values we can get without new queries
- A – if we want the new edge to extend T, we need $\tilde{\alpha} \in A$
- B – if the new edges should end in G, we need $\tilde{\alpha} \oplus \pi(\tilde{\alpha}) \in B$

Claim

If there is a collision in $\tilde{G}$ then $\tilde{\alpha} \in A$ and $\tilde{\alpha} \oplus \pi_1(\tilde{\alpha}) \in B$ with high probability

Claim

The collision point Δ with high probability is already in G (is not generated by the expansion).

Assume otherwise. This means that the final vertex is created during the expansion process by the R1 query $\tilde{\alpha}$. There would be two values $\alpha'_i, \alpha'_j \in R_2$ such that

$$\Delta = \tilde{\alpha} \oplus \pi_1(\tilde{\alpha}) \oplus \alpha'_i \oplus \pi_2(\alpha'_i) = \tilde{\alpha} \oplus \pi_1(\tilde{\alpha}) \oplus \alpha'_j \oplus \pi_2(\alpha'_j) = \Delta$$

so

$$\alpha'_i \oplus \pi_2(\alpha'_i) = \alpha'_j \oplus \pi_2(\alpha'_j)$$

and probability of this happening is upper bounded by $q_2^2/2^n$.

Returning path

- Consider the path that leaves (for a while) G.
- Since $\Delta \in G$ with high prob., the end of the path is in G.
- Go from IV forward and find the edge (Δ_b, Δ_{b+1}) such that $\Delta_b \in G$, and $\Delta_{b+1} \notin G$
- Edge (Δ_b, Δ_{b+1}) was created during the expansion, so there exists $\alpha' \in R_2$ such that $\tilde{\alpha} \oplus \alpha' = \Delta_b$ and thus $\tilde{\alpha} \in A$.
- Go from Δ backwards and find the edge (Δ_{a-1}, Δ_a) where $\Delta_{a-1} \notin G$ and $\Delta_a \in G$
- Edge (Δ_{a-1}, Δ_a) was created during the expansion, so there must be $\alpha'_j \in R_2$ such that $\Delta_{a-1} = \tilde{\alpha} \oplus \alpha'_j$ and $\Delta_a = \tilde{\alpha} \oplus \pi_1(\tilde{\alpha}) \oplus \alpha'_j \oplus \pi_2(\alpha'_j)$ and so $\tilde{\alpha} \oplus \pi_1(\tilde{\alpha}) \in B$

$$
\begin{aligned}
P &= \frac{|B|}{2^n - q_1} \quad \text{//to get a coll. we need to hit } B \text{ with new query} \\
&= \frac{|V| \cdot q_2}{2^n - q} \quad \text{//from the def. of } B \\
&\leq \frac{2 \cdot |V| \cdot q_2}{2^n} \quad \text{//assuming } q < 2^{n-1} \text{ ??} \\
&\leq \frac{2 \cdot (2q_1q_2 + 1) \cdot q_2}{2^n} \quad \text{// } |V| \leq 2q_1q_2 + 1 \\
&= \frac{2 \cdot (2(q - q_2)q_2 + 1) \cdot q_2}{2^n} \quad \text{//} \max_{0 \leq x \leq q} x \mapsto 2((q-x)x+1)x \approx 2/3q \\
&\leq \frac{2 \cdot q^3}{3 \cdot 2^n}
\end{aligned}
$$

At q-th step the probability is lower than $q^3/2^n + q^2/2^n$, so in the end after Q steps we have

$$
\sum_{q=1}^{Q} \left(q^3/2^n + q^2/2^n\right) \leq 2Q^4/2^n
$$

Proposition

For $Q \geq 2^{3n/8} + 2$ there exists a computationally unbounded adversary with high success probability.

Attack scenario

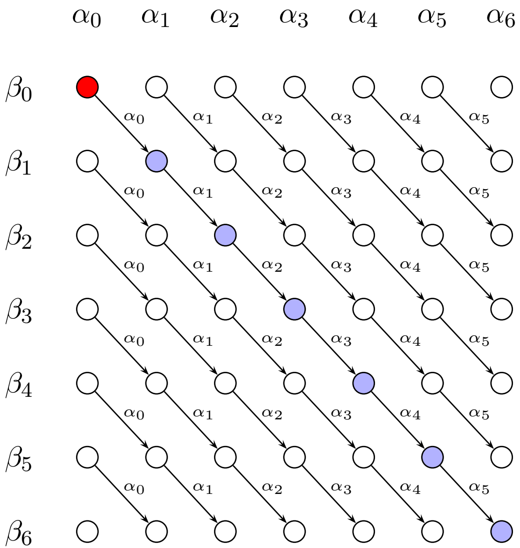
Algorithm:

- Pick α_0 randomly and set $\beta_0 \leftarrow \alpha_0 \oplus IV$
- Generate the sequences $(\alpha_i)_{0 \le i \le q}$, $(\beta_i)_{0 \le i \le q}$ as
  - $\alpha_i = \alpha_{i-1} \oplus \pi_1(\alpha_{i-1})$, $i = 1, \ldots, q$
  - $\beta_i = \beta_{i-1} \oplus \pi_2(\beta_{i-1})$, $i = 1, \ldots, q$
- compute $(q+1)^2$ values $\Delta_{i,j} = \alpha_i \oplus \beta_j$
- Look for different paths that start in IV and end in the same node

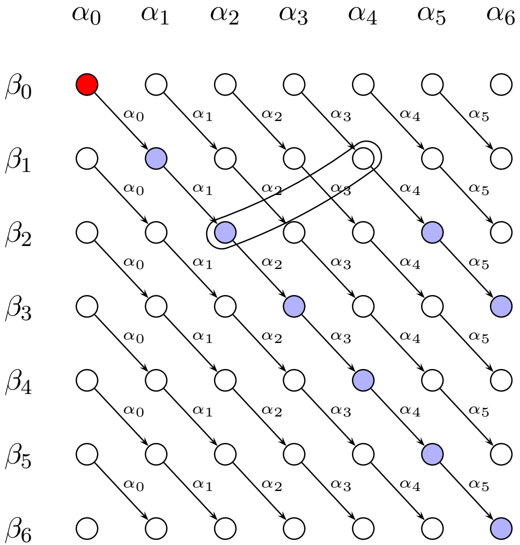
Important properties:

- $f(\Delta_{i,i}, \alpha_i) = \Delta_{i+1,i+1}$ for all $0 \le i \le q$
- $f(\Delta_{i,j}, \alpha_i) = \Delta_{i+1,j+1}$ for all $0 \le i, j \le q$

where f is the compression function



α_0 α_1 α_2 α_3 α_4 α_5 α_6
β_0
β_1
β_2
β_3
β_4
β_5
β_6



- $k = 2, i = 4, j = 1$ colliding triplet
- Tree grows by 2 nodes

Estimate the size of the tree

$$Set = \{(i,j,k) : i \neq j, i \neq k, j \neq k\}, \quad //|Set| = (q+1)q(q-1)$$

$$t \approx 1 + q + \sum_{(i,j,k) \in Set} \mathbf{1}_{[\Delta_{k,k} = \Delta_{i,j}]}(q - \max(i,j))$$

$$E[t] \approx 1 + q + \sum_{(i,j,k) \in Set} Pr[\Delta_{k,k} = \Delta_{i,j}](q - \max(i,j))$$

Assume $Pr[\Delta_{k,k} = \Delta_{i,j}] = 1/2^n$

$$E[t] \approx 1 + q + 1/2^n \cdot \sum_{(i,j,k) \in Set} (q - \max(i,j))$$

The fomula in the paper is slightly wrong, it should be

$$1 + q + \frac{q(q+1) \cdot (q-1)(q-1)}{3 \cdot 2^n} \approx \frac{q^4}{3 \cdot 2^n}$$

$k=0$	$i=0$	$i=1$	$i=2$	$i=3$
$j=0$	3	2	1	0
$j=1$	2	2	1	0
$j=2$	1	1	1	0
$j=3$	0	0	0	0

$k=1$	$i=0$	$i=1$	$i=2$	$i=3$
$j=0$	3	2	1	0
$j=1$	2	2	1	0
$j=2$	1	1	1	0
$j=3$	0	0	0	0

$k=2$	$i=0$	$i=1$	$i=2$	$i=3$
$j=0$	3	2	1	0
$j=1$	2	2	1	0
$j=2$	1	1	1	0
$j=3$	0	0	0	0

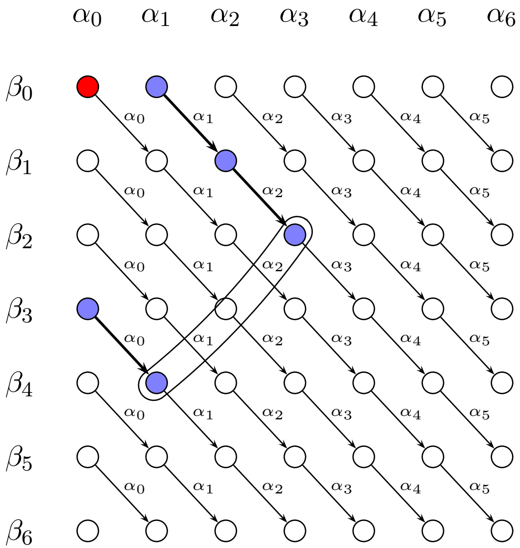
$k=3$	$i=0$	$i=1$	$i=2$	$i=3$
$j=0$	3	2	1	0
$j=1$	2	2	1	0
$j=2$	1	1	1	0
$j=3$	0	0	0	0

Closed form of the sum

$$\sum_{(k,i,j)\in Set} (q - \max(i,j))$$

- Sum of all elements in each plane is $\sum_{u=0}^{q} u^2 = u(u+1)(2u+1)/6$
- Diagonal never counts so we have $\sum_{u=0}^{q} u^2 - \sum_{u=0}^{q} u$
- There are $q+1$ planes and each element is excluded from exactly two planes because of $i \neq k$, $j \neq k$
- Total: $(q-1)\frac{u(u+1)(2u+1)-3u(u+1)}{6}$

Compression function collisions in $2^{l/4}$ queries



- After q queries we have $q^2/4$ hash nodes
- To find a collision among them, we need $q^2/4 \approx \sqrt{2\pi} \cdot 2^{l/2}$
- This means we can find a compression function collision in $q \approx 2^{l/4+3}$ queries
- Real complexity higher