How to use differential trails to attack compression functions

Joan Daemen, Jonhathan Fuchs and Yann Rotella
Dagstuhl, Germany

January 21, 2020

UNIVERSITÉ DE VERSAILLES
ST-QUENTIN-EN-YVELINES

Structure of this Talk

The Serial Construction

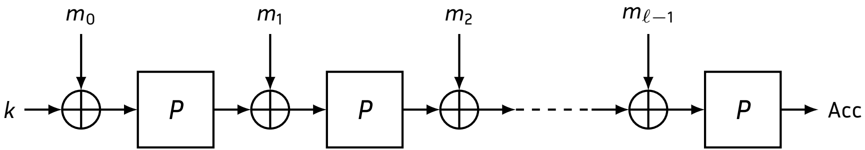


Figure: The Serial Construction

Parallel Construction

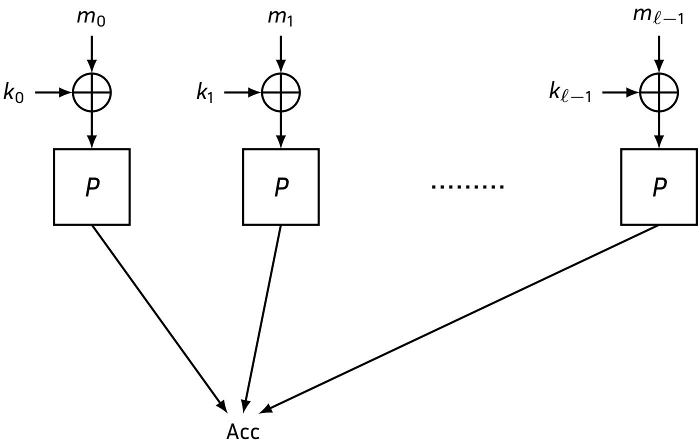
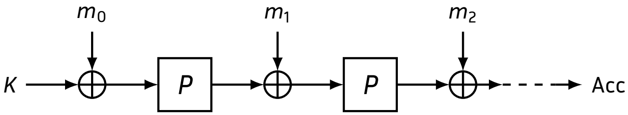
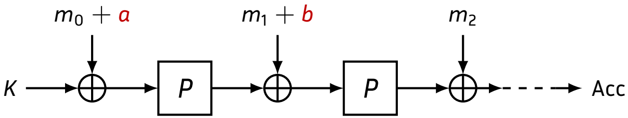
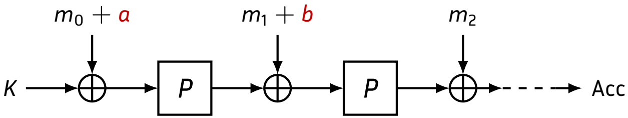


Figure: The Parallel Construction

Plan of this Section

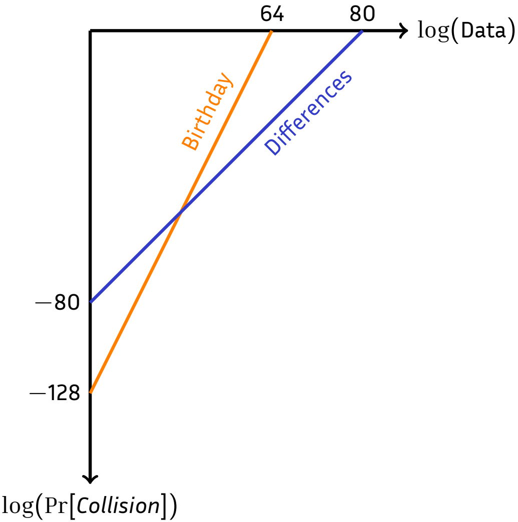

m_0
m_1
m_2
K
P
P
Acc


$m_0 + a$
$m_1 + b$
m_2
K
P
P
Acc

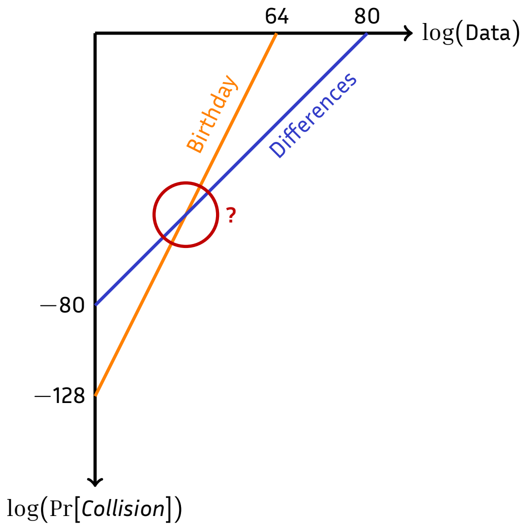


$$\Pr[\mathit{Collision}] = \mathsf{DP}(a, b)$$

Birthday VS Difference



Birthday VS Difference



Using Covering Vector spaces

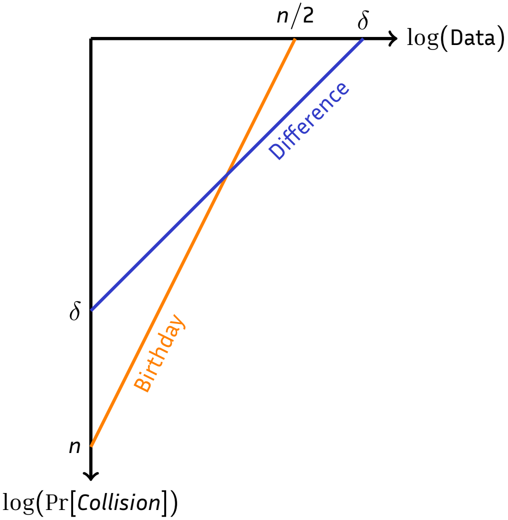
$\langle (a_1, b_1), (a_2, b_2), \ldots, (a_v, b_v) \rangle = V$ such that

$$\sum_{(a,b)\in V} \delta_{a,b} > \delta\,.$$

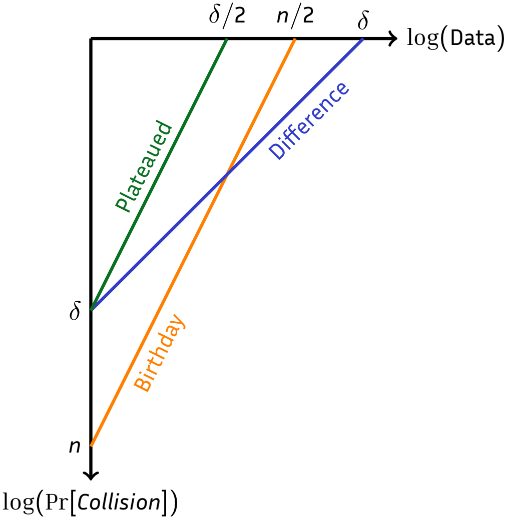
By making this strategy:

$$\boxed{\begin{array}{c} M_0, M_1 \\ M_0 + a_1, M_1 + b_1 \\ M_0 + a_2, M_1 + b_2 \\ M_0 + a_1 + a_2, M_1 + b_1 + b_2 \\ \vdots \\ M_0 + \sum a_i, M_1 + \sum b_i \end{array}} \quad \boxed{\begin{array}{c} M'_0, M'_1 \\ M'_0 + a_1, M'_1 + b_1 \\ M'_0 + a_2, M'_1 + b_2 \\ M'_0 + a_1 + a_2, M'_1 + b_1 + b_2 \\ \vdots \\ M'_0 + \sum a_i, M'_1 + \sum b_i \end{array}} \quad \ldots\ldots\ldots$$

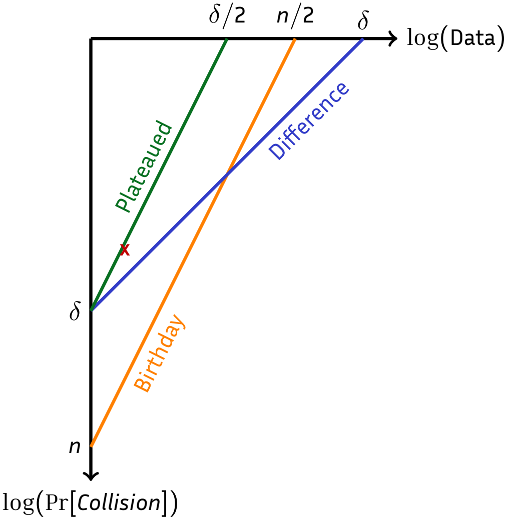
In terms of Security



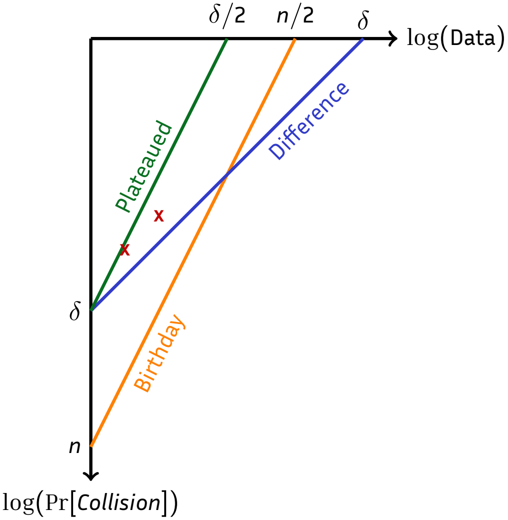
In terms of Security



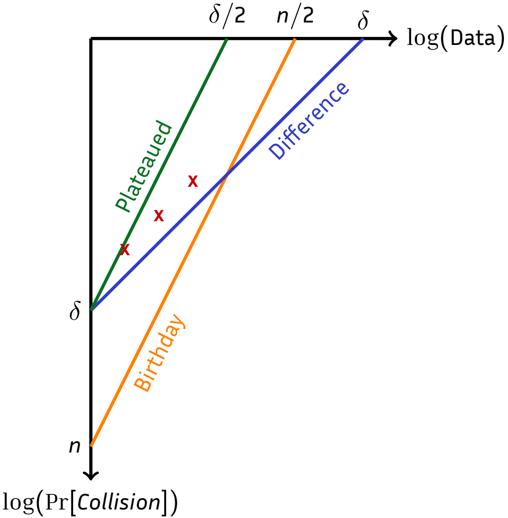
In terms of Security



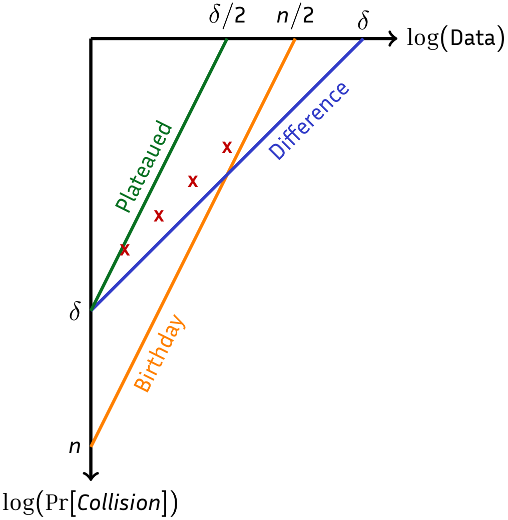
In terms of Security



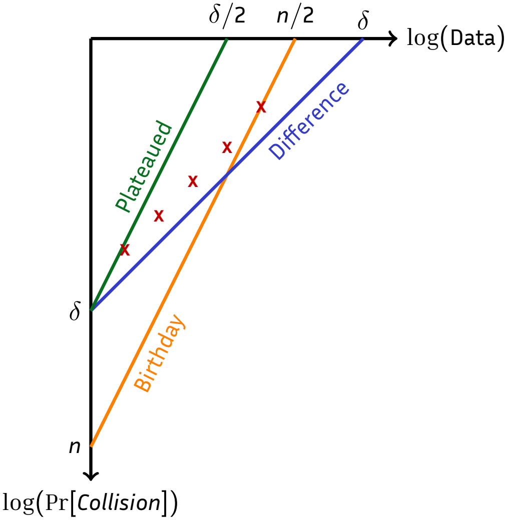
In terms of Security



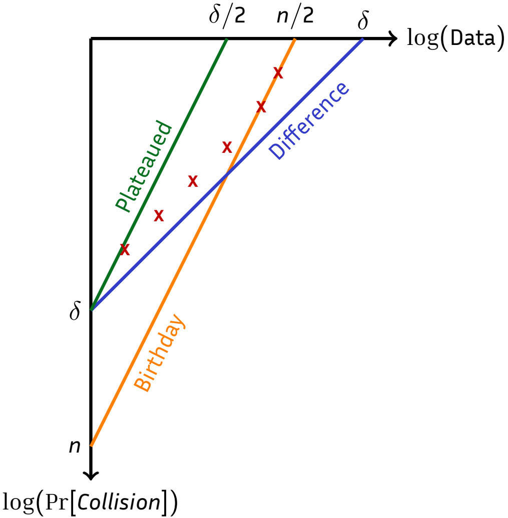
In terms of Security



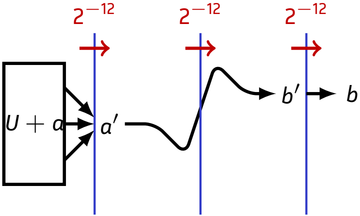
In terms of Security



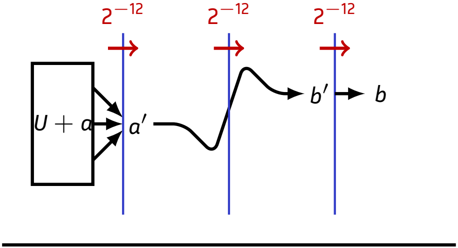
In terms of Security



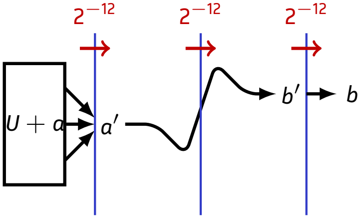
In Practice: XooDoo

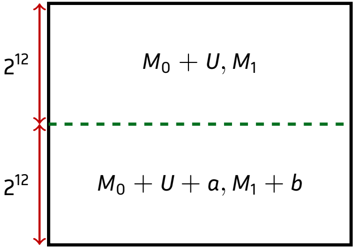


In Practice: XooDoo

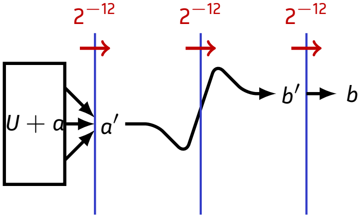


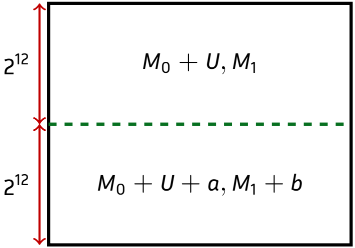
In Practice: XooDoo





In Practice: XooDoo

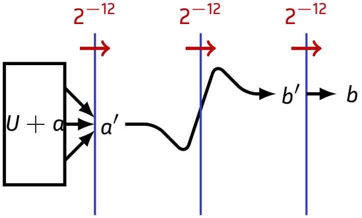


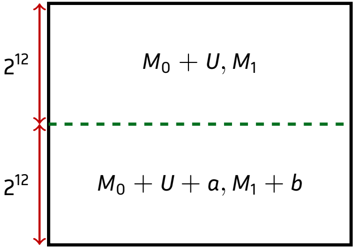


Number of pairs st a': 2^{12}

$$\Pr[Collision] = 2^{12} \times 2^{-24}$$

In Practice: XooDoo

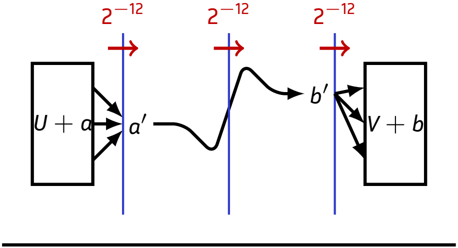




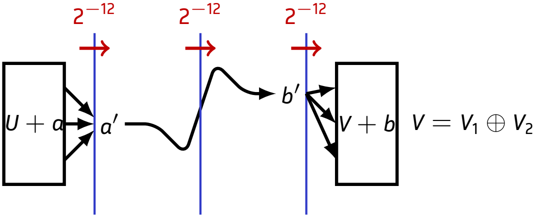
Number of pairs st a': 2^{12}

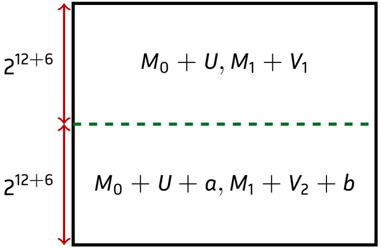
$$\begin{aligned}\Pr[Collision] &= 2^{12} \times 2^{-24} \\ &= 2^{-12}\end{aligned}$$

In Practice: XooDoo

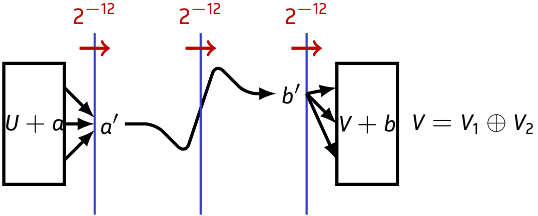


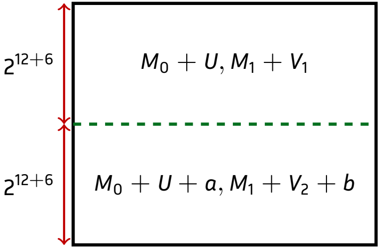
In Practice: XooDoo





In Practice: XooDoo

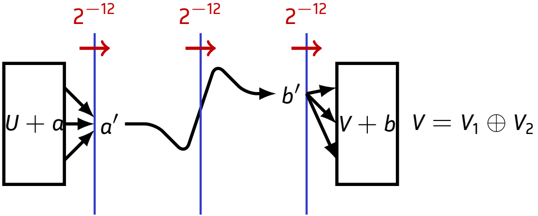


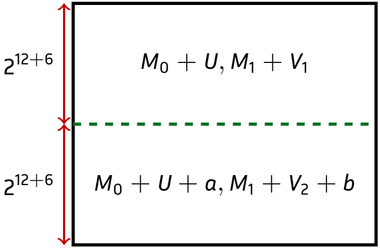


Number of pairs st a': 2^{12}

Catching b': $2^{12} \times 2^{-12} = 1$

In Practice: XooDoo





Number of pairs st a': 2^{12}

Catching b': $2^{12} \times 2^{-12} = 1$

Win wp. 1 with 2^{19}.

Security Criteria

If trail $a \mapsto b$ with probability $2^{-w_1 - w_2 - w_3 \cdots - w_r}$, we get collision with probability

Security Criteria

If trail $a \mapsto b$ with probability $2^{-w_1-w_2-w_3\cdots-w_r}$, we get collision with probability

$$2^{w_1-w_2-w_3-\cdots-w_{r-1}}$$

using

$$D = 2^{1+w_1+w_r/2}$$

We gain the first round and the half of the last round

Plan of this Section

New Criteria: Squared pseudo-Walsh Coefficient

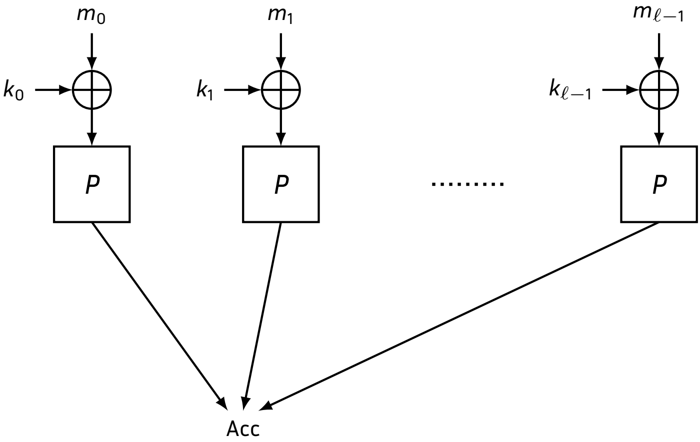


Figure: The Parallel Construction

Results

If Keys are independent and uniformly distributed, then

$$\Pr[F(M) = F(M')|M + M' = \Delta]$$

is maximal when Δ has the same value on two blocks exactly.

Results

If Keys are independent and uniformly distributed, then

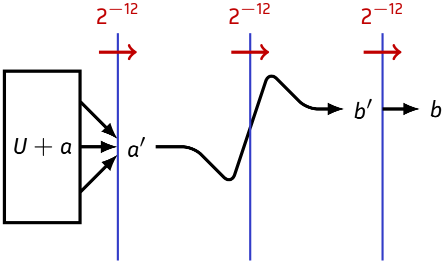
$$\Pr[F(M) = F(M')|M + M' = \Delta]$$

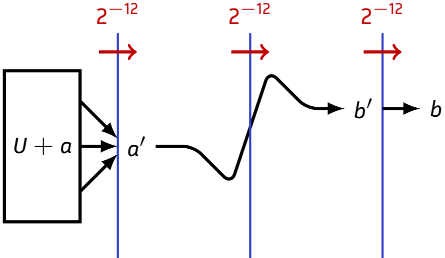
is maximal when Δ has the same value on two blocks exactly.

The relevant criteria is

$$\max_a \sum_b (\mathrm{DP}(a, b))^2$$

In iterated construction





Security Criteria

- Complexity: $2^{2w_1+2w_2+\cdots+2w_{r-1}+w_r}$.

Plan of this Section

Conclusion

Both strategies share the same security criteria:

- The first round doesn't count;
- The last round counts for half.

But...

Conclusion

Both strategies share the same security criteria:

- The first round doesn't count;
- The last round counts for half.

But... The parallel strategy seems to offer twice the security.