Links Between Theoretical and Effective Differential Probabilities: Experiments on PRESENT

Céline Blondeau, Benoît Gérard*

SECRET-Project-Team, INRIA, France

TOOLS for Cryptanalysis - 23th June 2010

Outline

Outline

Notation

We consider iterative block ciphers (especially PRESENT)

- operating on m-bit messages;
- using a master key K;
- with round function F using subkeys K_i;

$$Y \stackrel{\text{def}}{=} \text{Enc}_K(X) \stackrel{\text{def}}{=} F_{K_r} \circ F_{K_{r-1}} \circ \cdots \circ F_{K_1}(X).$$

We focus on the particular case of key alternating ciphers.

Differential

A *r*-round differential of a cipher is a couple

$$(\delta_0, \delta_r) \in \mathbb{F}_2^m \times \mathbb{F}_2^m.$$

The probability of a *r*-round differential is

$$p_* \stackrel{\text{def}}{=} \Pr_{\mathbf{X},\mathbf{K}} \left[\mathrm{Enc}_K(X) \oplus \mathrm{Enc}_K(X \oplus \delta_0) = \delta_r \right].$$

If $p_* > 2^{-m}$, then we can distinguish F_K^r from a random permutation.

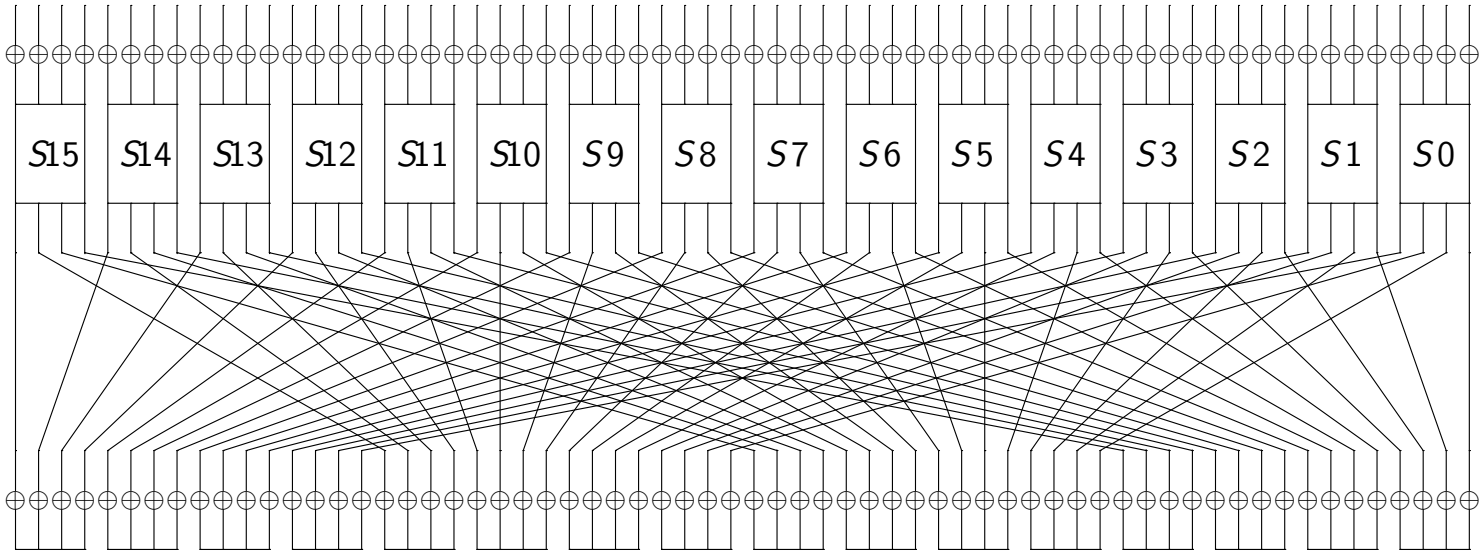
$$\Downarrow$$

Statistical Cryptanalysis.

PRESENT

A 64-bit block cipher presented in [Bogdanov *et al.*, CHES 2007].

- 80-bit or 128-bit key schedule.
- Substitution Permutation Network (SPN).
- A single 4-bit Sbox.



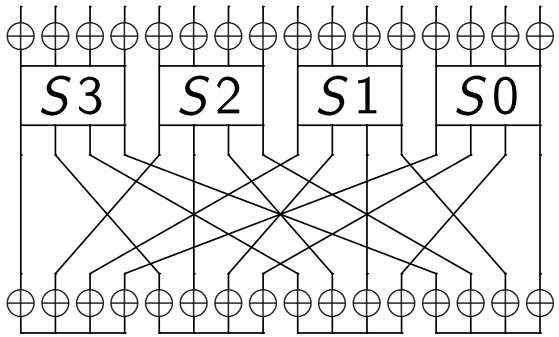
SMALLPRESENT-[s]

Proposed by Leander in 2009.

- s is the number of Sboxes thus SMALLPRESENT-[s] is a $4\,s$-bit cipher.
- The permutation is similar to the one of PRESENT.
- 80-bit key schedule.

All of the experiments but one are done on SMALLPRESENT-[4].

One round of SMALLPRESENT-[4].



Key schedules

We introduced 2 other key schedules:

- a 16-bit key schedule (all subkeys are equal).
- a 20-bit key schedule (similar to the 80-bit one):
  - Master key: $K = k_{19}k_{18}\ldots k_0$.
  - Round keys: $K_i = k_{19}k_{18}\ldots k_4$.
  - Updated as follows:
    1. $[k_{19}k_{18}\ldots k_1k_0] = [k_6k_5\ldots k_8k_7]$;
    2. $[k_{19}k_{18}k_{17}k_{16}] = S[k_{19}k_{18}k_{17}k_{16}]$;
    3. $[k_7k_6k_5k_4k_3] = [k_7k_6k_5k_4k_3] \oplus \mathit{roundcounter}$.

In this presentation, shown results are obtained using this last one.

Outline

Differential trails

A differential trail of a cipher is a $(r+1)$-tuple $(\beta_0, \beta_1, \cdots, \beta_r) \in (\mathbb{F}_2^m)^{r+1}$ of intermediate differences.

The probability p_β of a differential trail $\beta = (\beta_0, \beta_1, \cdots, \beta_r)$ is:

$$p_\beta \stackrel{\text{def}}{=} \Pr_{\mathbf{X},\mathbf{K}}\left[\forall i \;\; F_K^i(X) \oplus F_K^i(X \oplus \beta_0) = \beta_i\right].$$

If the cipher is Markov and the round subkeys are independent, then,

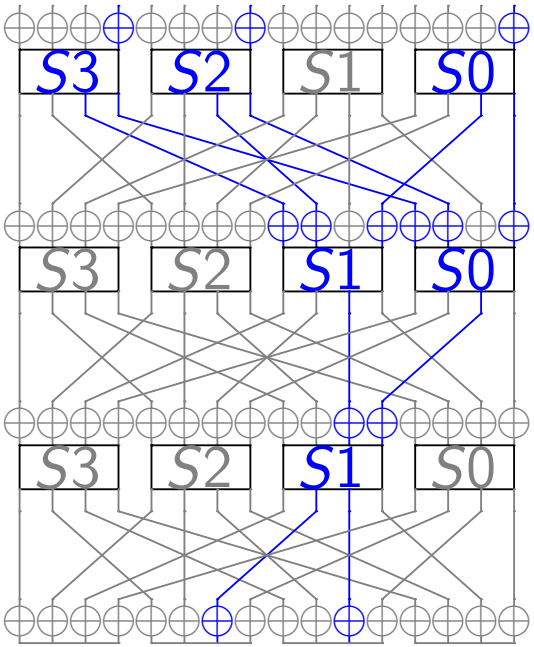
$$p_\beta^t \stackrel{\text{def}}{=} \prod_{i=1}^{r} \Pr_{\mathbf{X}}\left[F(X) \oplus F(X \oplus \beta_{i-1}) = \beta_i\right].$$

Key dependency (1/3)

For a differential trail β:

$$T_K \stackrel{\text{def}}{=} \frac{1}{2} \#\left\{X | F_K^i(X) \oplus F_K^i(X \oplus \beta_0) = \beta_i, \forall 1 \leq i \leq r\right\},$$

$$p_\beta = 2^{-(m-1)} \cdot \mathbb{E}(T_K).$$

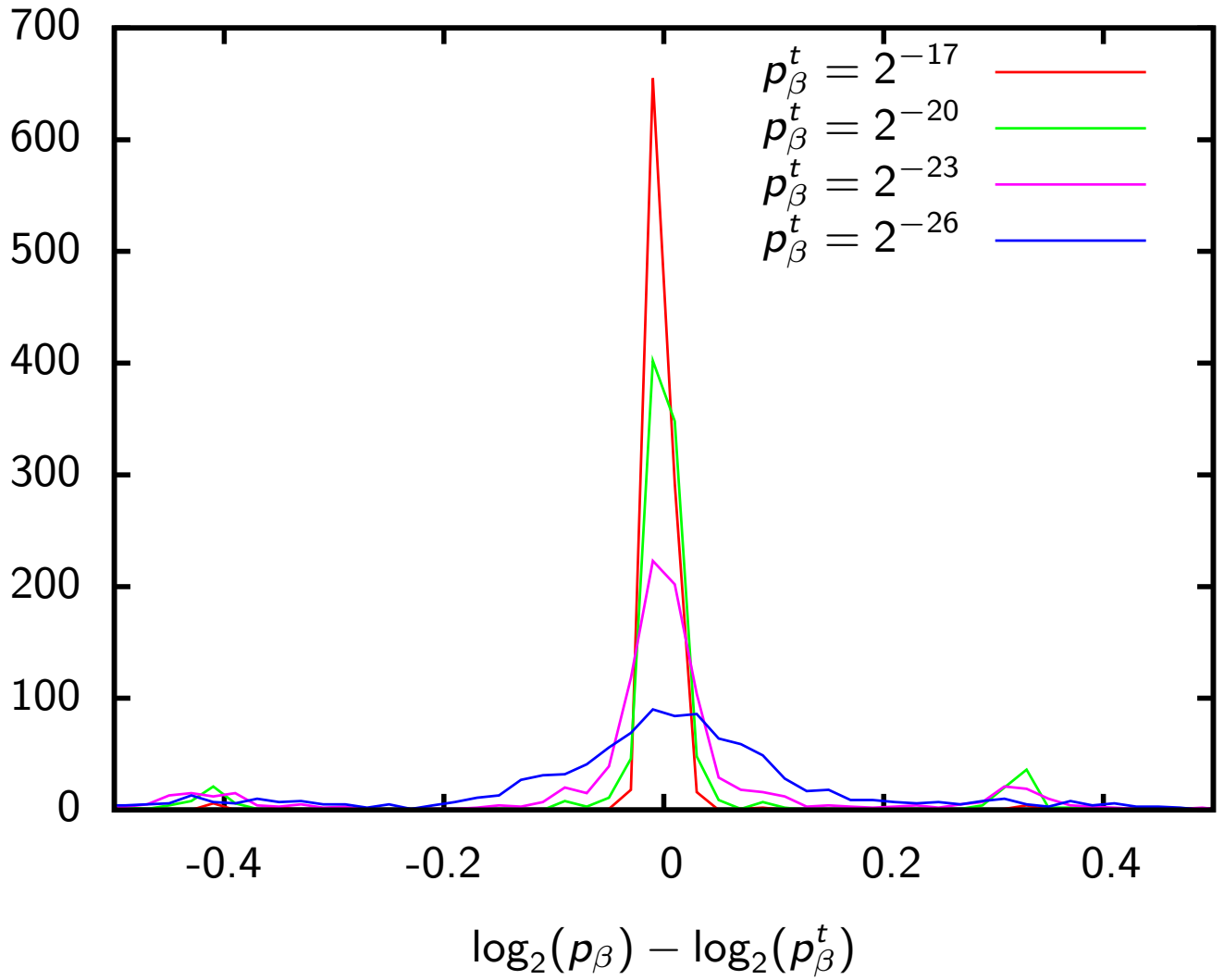


$$p_\beta^t = 8 \cdot 2^{-(16-1)}$$

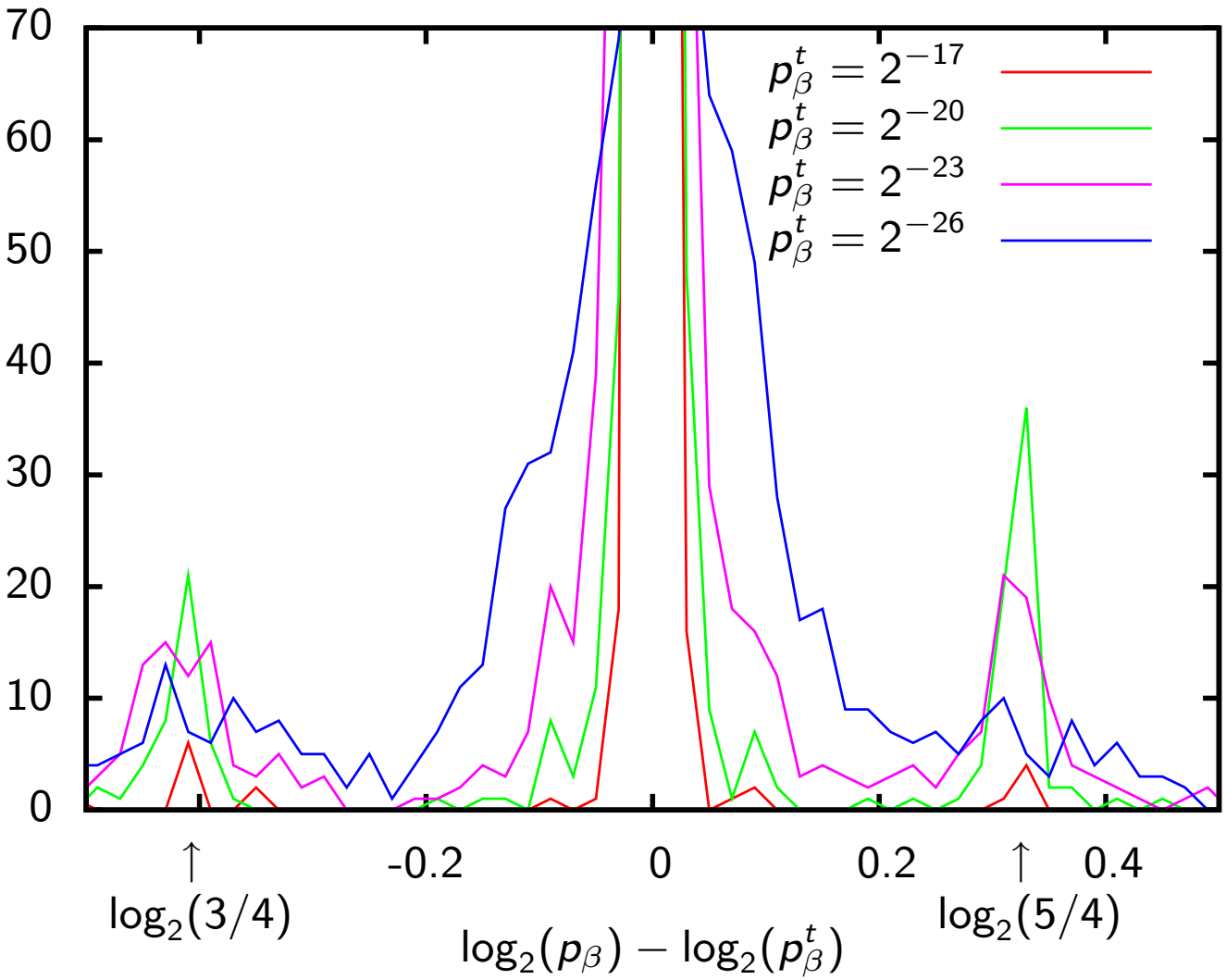
T_K	0	8	16
#	131072	524288	393216

$$p_\beta = 10 \cdot 2^{-(16-1)}.$$

Key dependency (2/3)

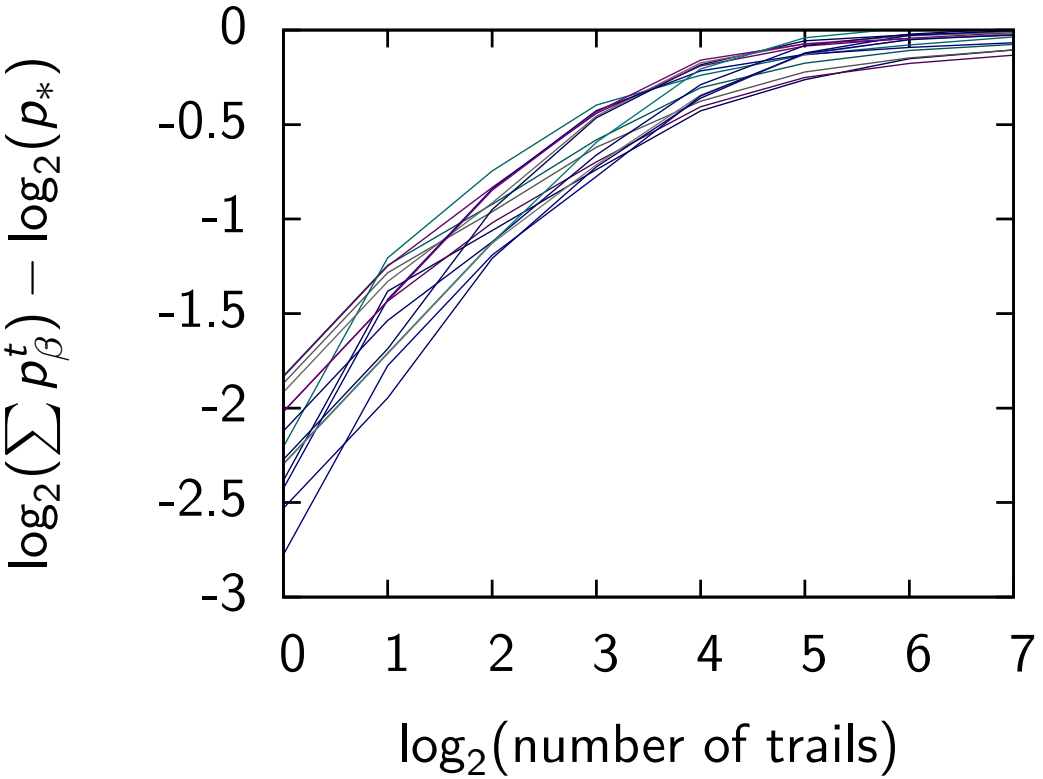


Key dependency (3/3)



Outline

Differential probability



The probability p_* of a r-round differential (δ_0, δ_r) is

$$p_* = \sum_{\beta=(\delta_0,\beta_1,\ldots,\beta_{r-1},\delta_r)} p_\beta.$$

Algorithm used: adaptation of [Biryukov et al., CRYPTO 2004].

Remarks on [Wang, AFRICACRYPT 2008]

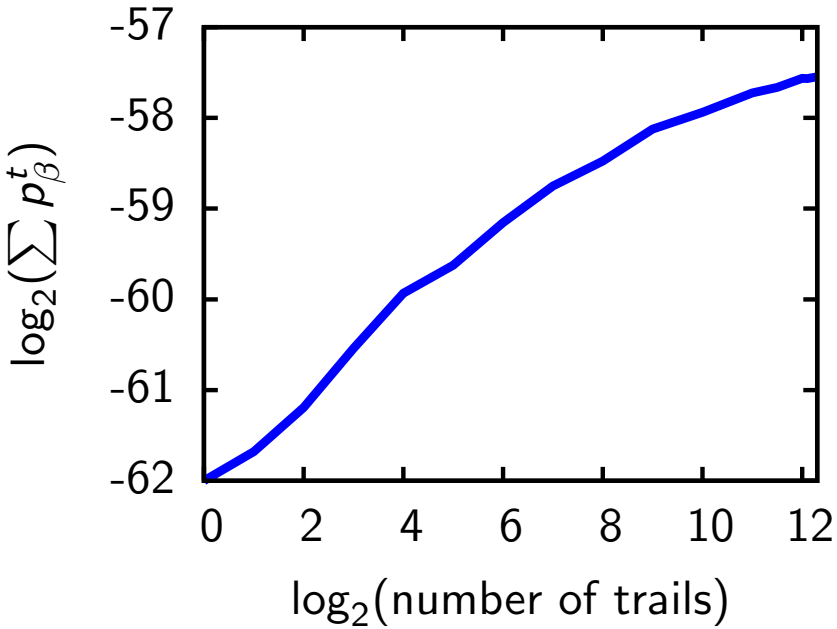
Attack:

- 14-round differentials with probability (lower bounded by) 2^{-62}.
- Obtained by iterating 3 times a 4-round differential trail.

Remarks:

- 2^{-62} is the best probability for a 14-round differential trail.
- Considering the $2^{12.2}$ best trails of the difference ($p_\beta^t \geq 2^{-73}$).

$$p_*^t = 2^{-57.53} \gg 2^{-62}.$$

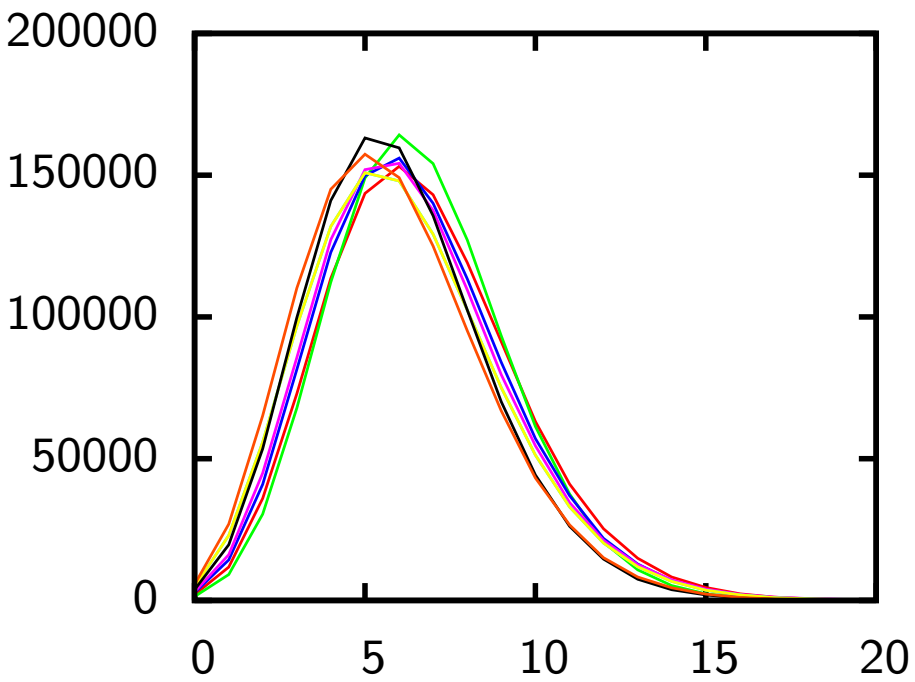


Key dependency

[Daemen, Rijmen 2005]

In the Sampling Model for key-alternating ciphers, variable D_K follows a **binomial distribution**.

$$D_K \stackrel{\text{def}}{=} \frac{1}{2}\#\{X | F_K^r(X) \oplus F_K^r(X \oplus \delta_0) = \delta_r\}.$$



Plots for 5-round differentials of SMALLPRESENT-[4].

Outline

Success Probability (1/2)

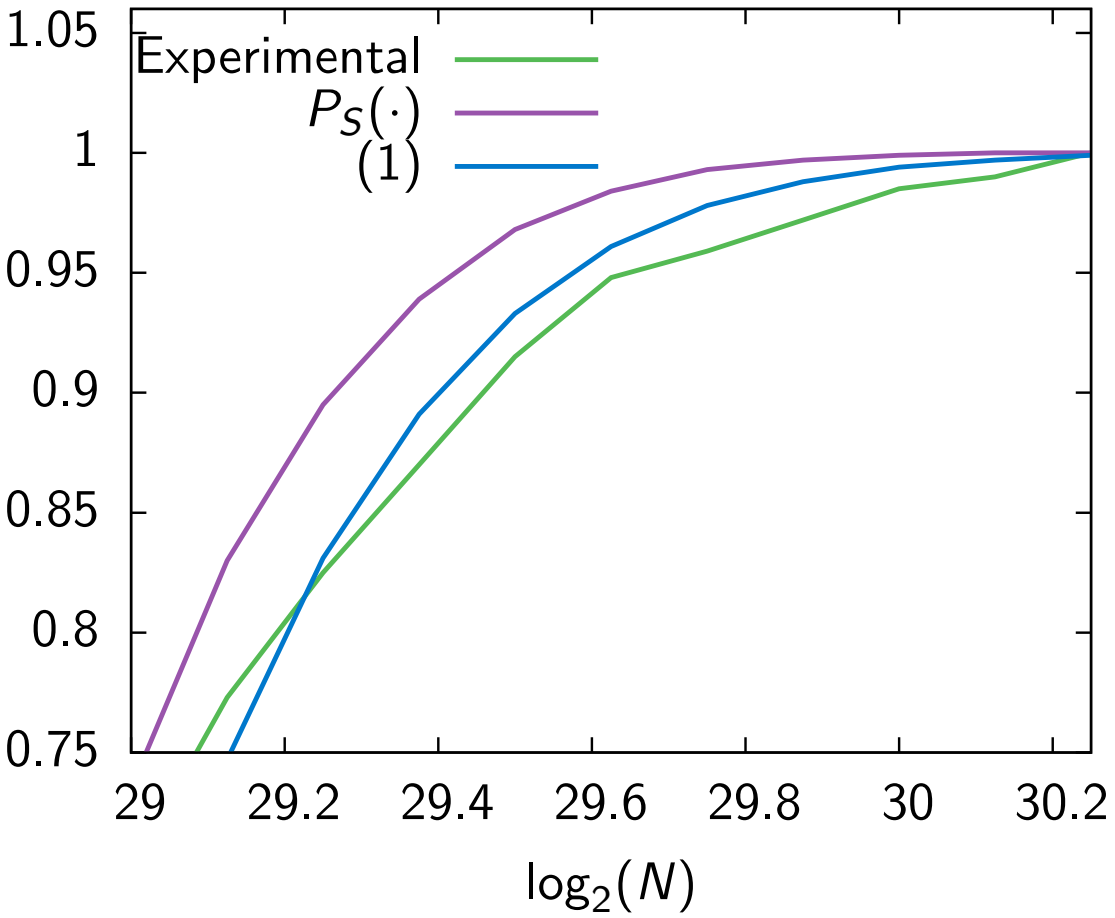
$$p_* \stackrel{\text{def}}{=} \Pr_{\mathbf{X},\mathbf{K}}\left[\mathrm{Enc}_K(X) \oplus \mathrm{Enc}_K(X \oplus \delta_0) = \delta_r\right].$$

The function $P_S(p)$ is the success probability of an attack with a fixed-key differential probability p.

The new formula for the Success Probability that takes into account the sampling model is:

$$\begin{aligned} P_{\text{success}} &\stackrel{\text{def}}{=} \mathbb{E}_{D_K}\left[P_S\left(\frac{D_K}{2^{m-1}}\right)\right] \\ &= \sum_{i=0}^{2^{m-1}} P_S\left(\frac{i}{2^{m-1}}\right) \cdot \left[(p_*)^i (1-p_*)^{2^{m-1}-i} \binom{2^{m-1}}{i}\right]. \quad (1) \end{aligned}$$

Success Probability (2/2)



- Differential attack,
- SMALLPRESENT-[8],
- 11 rounds,
- 2^{32} keys,
- 2^9 keys tried,
- 100 experiments.

Success Probability: choice of P_S (1/2)

[Selçuk, *Journal of Cryptology* 2007]

$$P_S \approx \int_{\Phi^{-1}(1-\frac{\ell}{n})}^{\infty} \phi_0(t)\, dt.$$

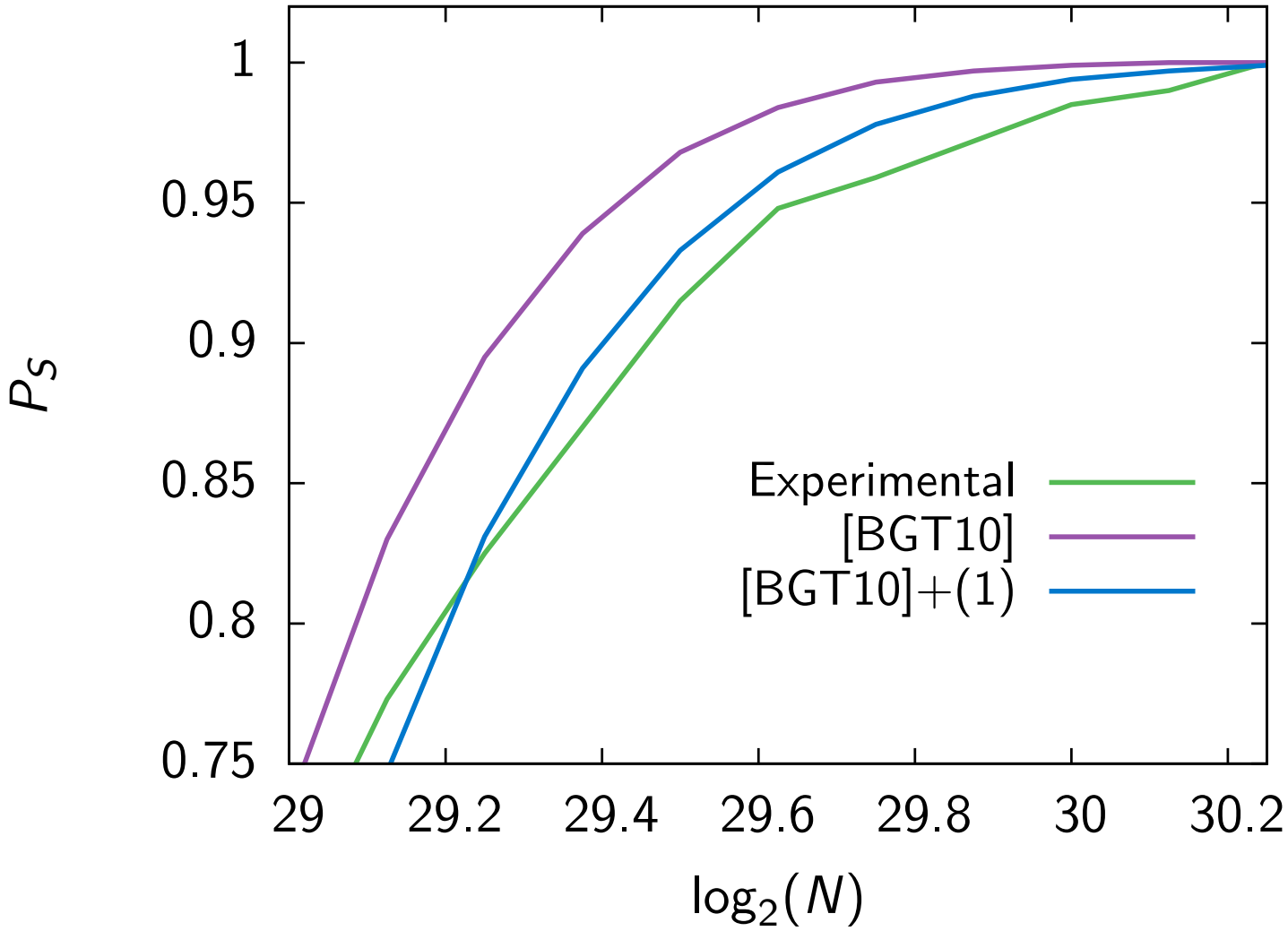
[Blondeau, Gérard and Tillich, *to appear in DCC*]

$$P_S \approx \sum_{i=F^{-1}\left(1-\frac{\ell-1}{n-2}\right)}^{N} P[X_0 = i].$$

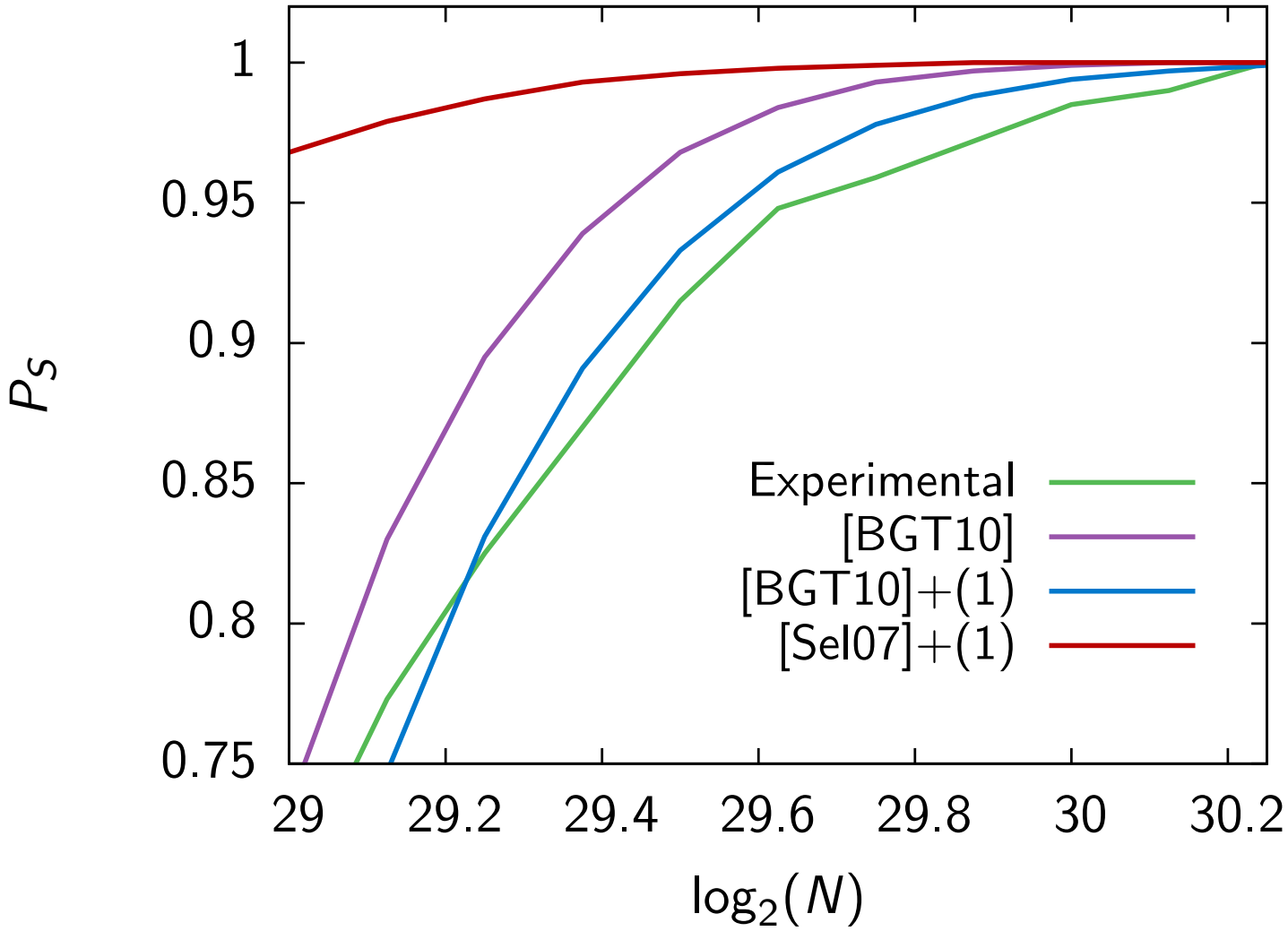
In the case of differential cryptanalysis,

THE SECOND ONE IS TIGHTER !!!

Success Probability: choice of P_S (2/2)



Success Probability: choice of P_S (2/2)

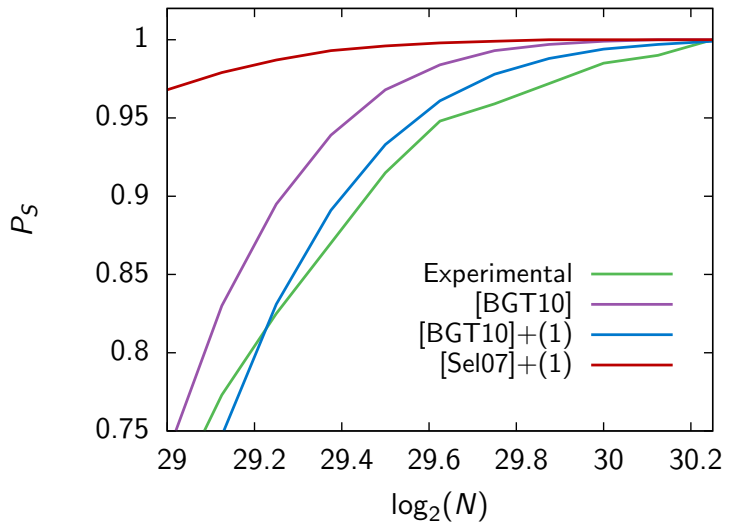


Recommendations

- Use more than one trail when estimating a differential probability.
  - For Wang's differential :

$$p_\beta \geq 2^{-64} \rightarrow 2^{-60.00} \quad : \quad \simeq 10s.$$
$$p_\beta \geq 2^{-66} \rightarrow 2^{-58.91} \quad : \quad \simeq 2m.$$
$$p_\beta \geq 2^{-70} \rightarrow 2^{-57.67} \quad : \quad \simeq 1h.$$
$$p_\beta \geq 2^{-73} \rightarrow 2^{-57.53} \quad : \quad \simeq 16h.$$

- Use the success probability formula given in this talk together with the one in [BGT10].



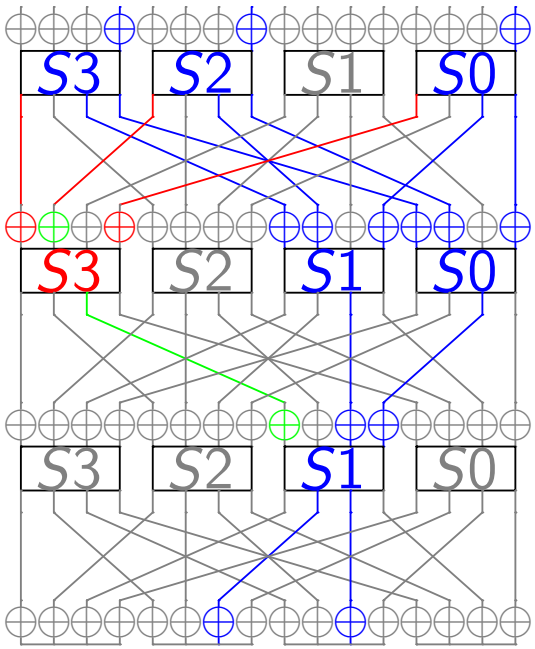
Conclusion and further work

- For most of the trails p_β^t seems to be a good estimate for p_β.
- Although p_β^t can be different from p_β, it seems that $\sum p_\beta^t \approx p_*$.
- The *Sampling Model* seems to be well suited at least in the case of SMALLPRESENT-[4] and SMALLPRESENT-[8].
- This leads to a new formula for the success probability of a differential attack.

Results are obtained on SMALLPRESENT-[4]

- Trying to run experiments on SMALLPRESENT-[8] to extrapolate on the full PRESENT.
- Running experiments on other SPNs or Feistel networks.

Explanation on the 3-round trail

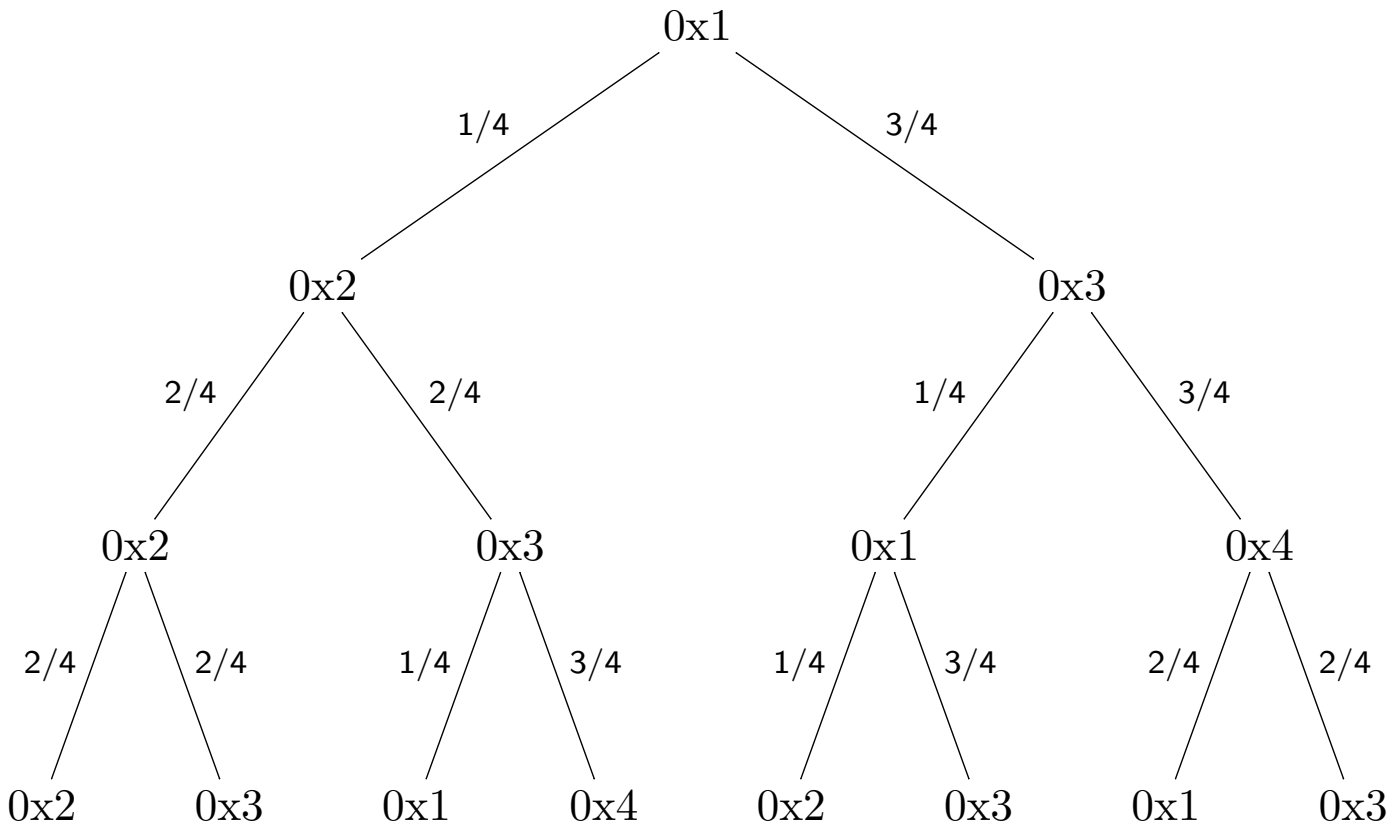


- 0x1 $\rightarrow$0x3 implies red bits to 0.
- 0x3 $\rightarrow$0x6 implies green bit to 1.
- Two green key bits correspond to the same master key bit.

Key bits	000	001	010	011
Probability of 1	1/2	1/2	1/2	1
Key bits	100	101	110	111
Probability of 1	1	1/2	1	0

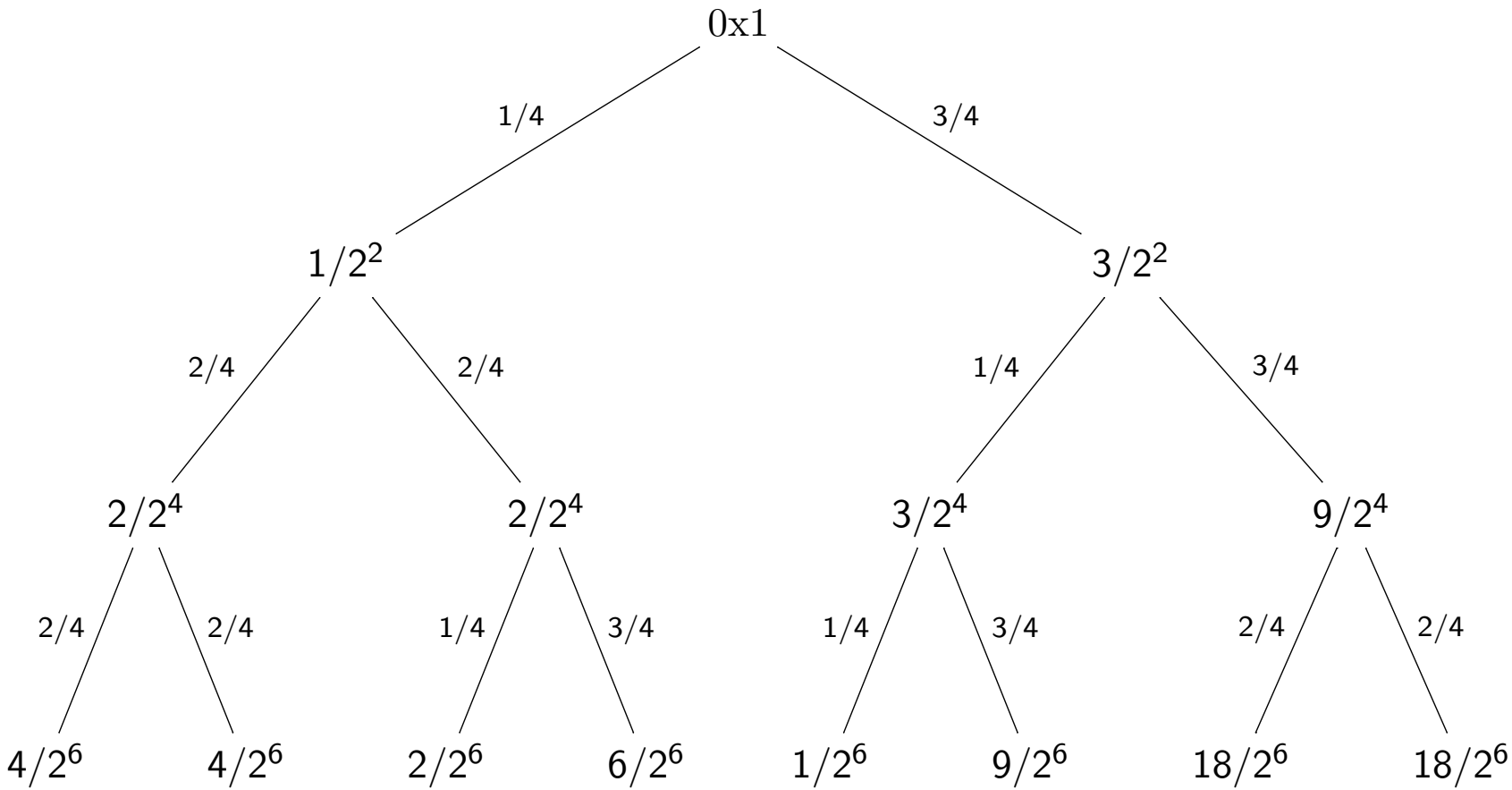
Finding differential trails

Finding trails with probability $> 10/2^6$.



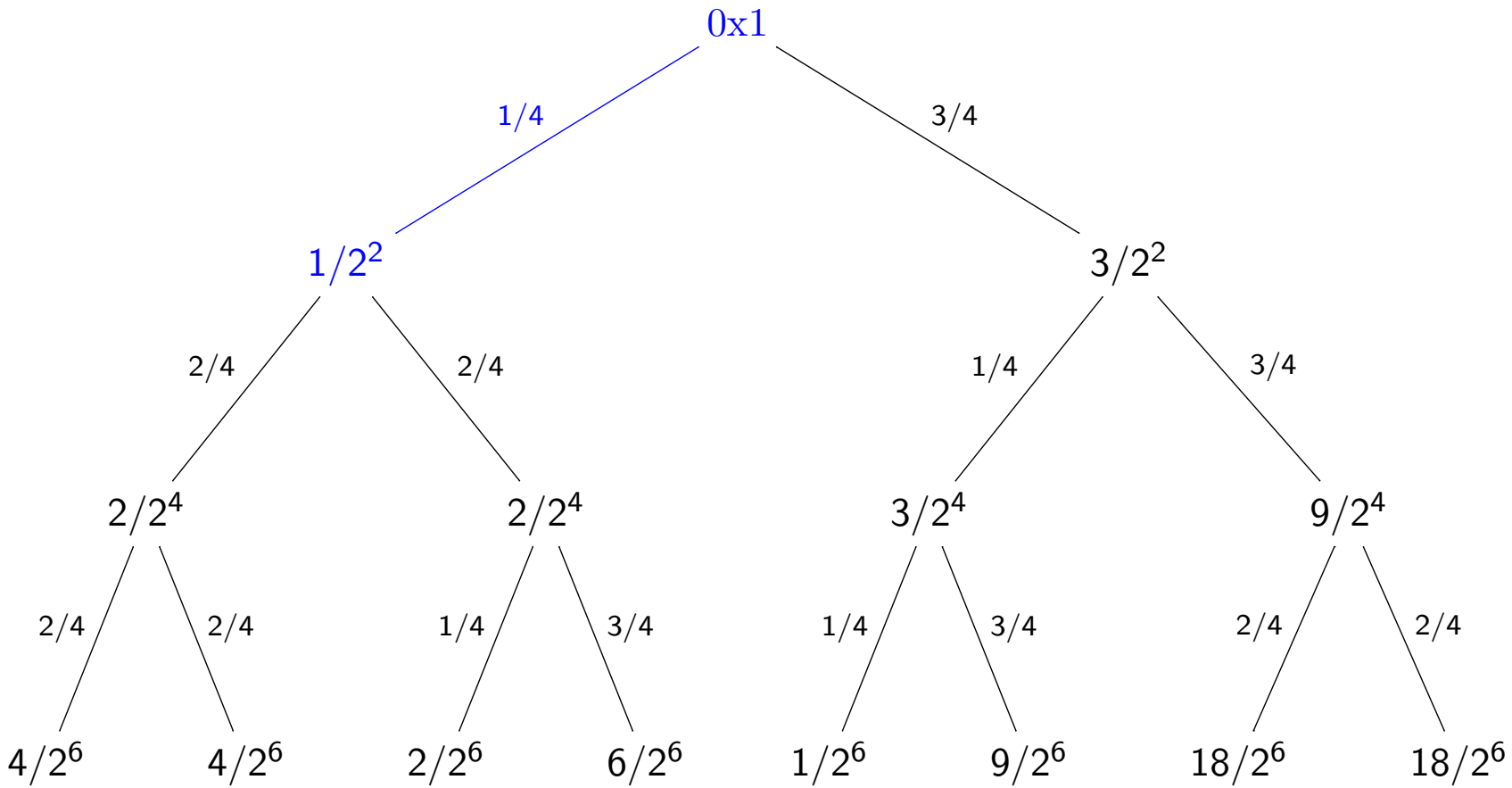
Finding differential trails

Finding trails with probability $> 10/2^6$.



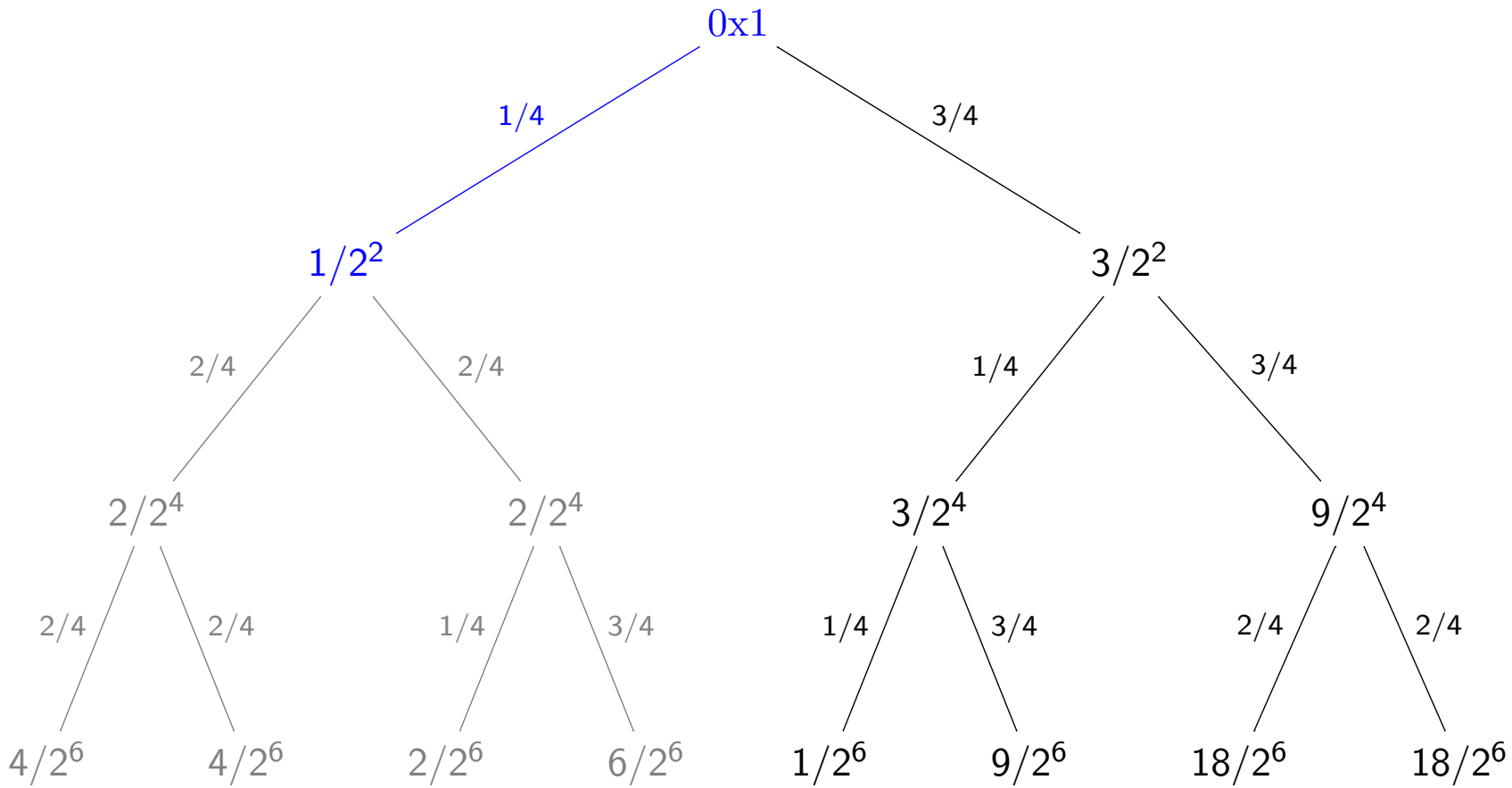
Finding differential trails

Finding trails with probability $> 10/2^6$.



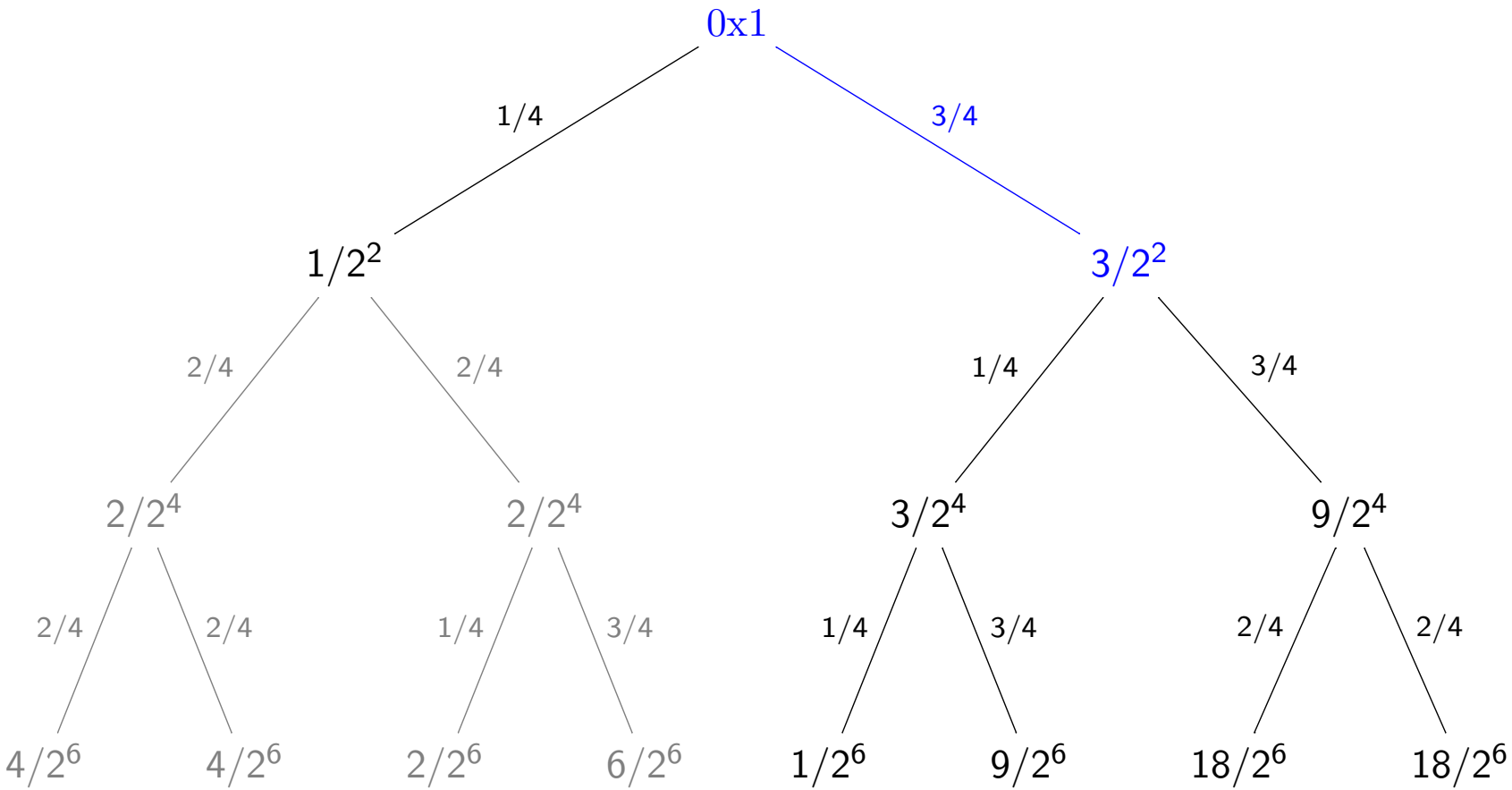
Finding differential trails

Finding trails with probability $> 10/2^6$.



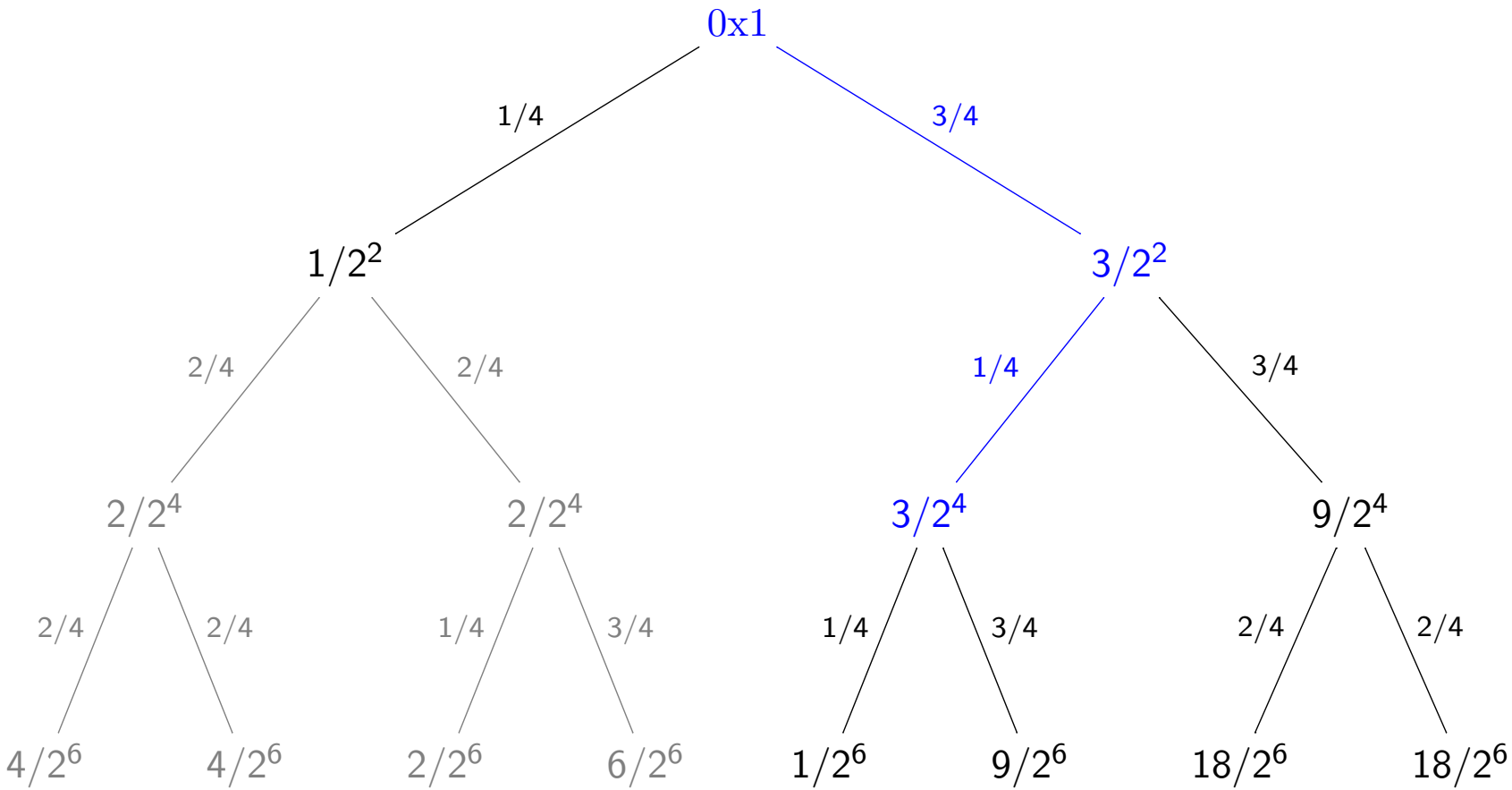
Finding differential trails

Finding trails with probability $> 10/2^6$.



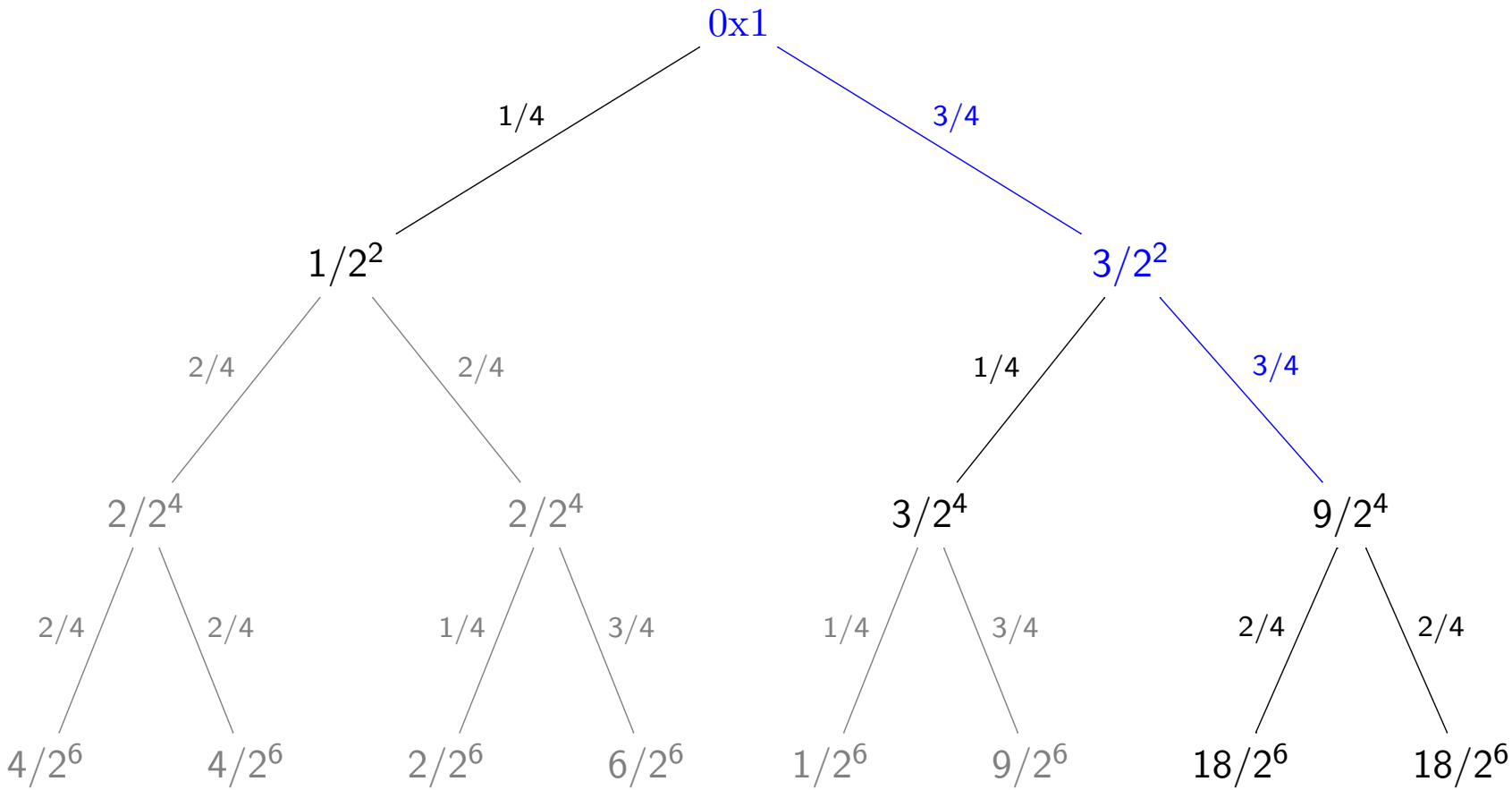
Finding differential trails

Finding trails with probability $> 10/2^6$.



Finding differential trails

Finding trails with probability $> 10/2^6$.



Finding differential trails

Finding trails with probability $> 10/2^6$.