New Circuit Minimization Techniques for Smaller and Faster AES SBoxes

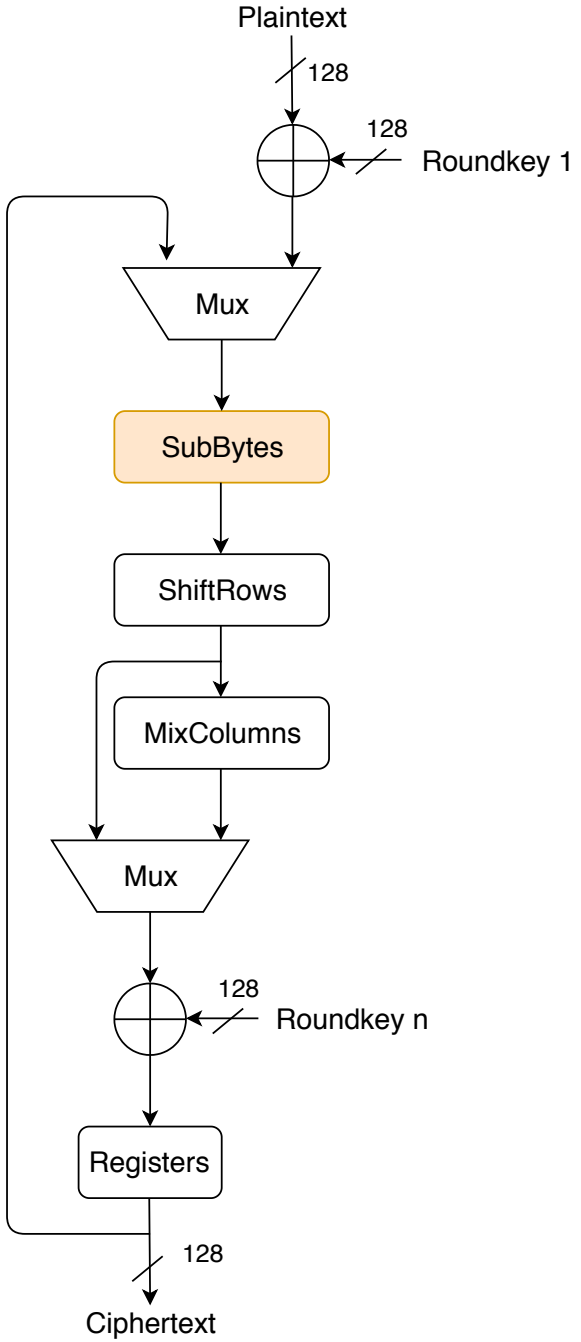
Alexander Maximov and Patrik Ekdahl
Ericsson Research

Preliminaries

AES Round Function

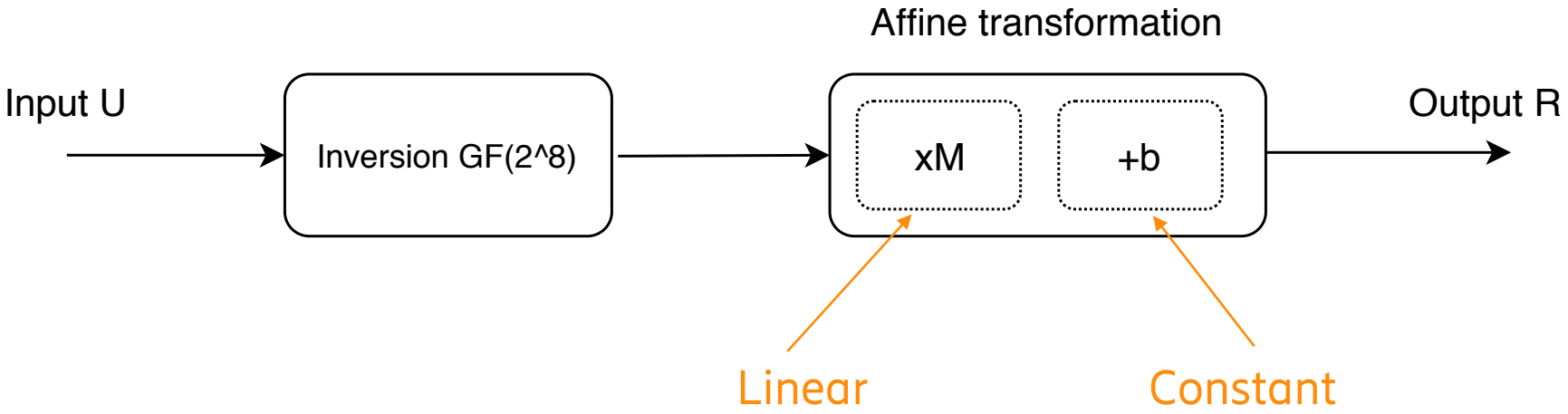
- SubBytes is the only non-linear part
- 16 8x8 SBoxes needed for a full implementation
- Forward only or combined SBox
- In ASICs
  - Look-up table
  - Gate implementation

What to remember:
— New improved methods for circuit minimization.
— New SBox architecture which improves the critical path.



Preliminaries

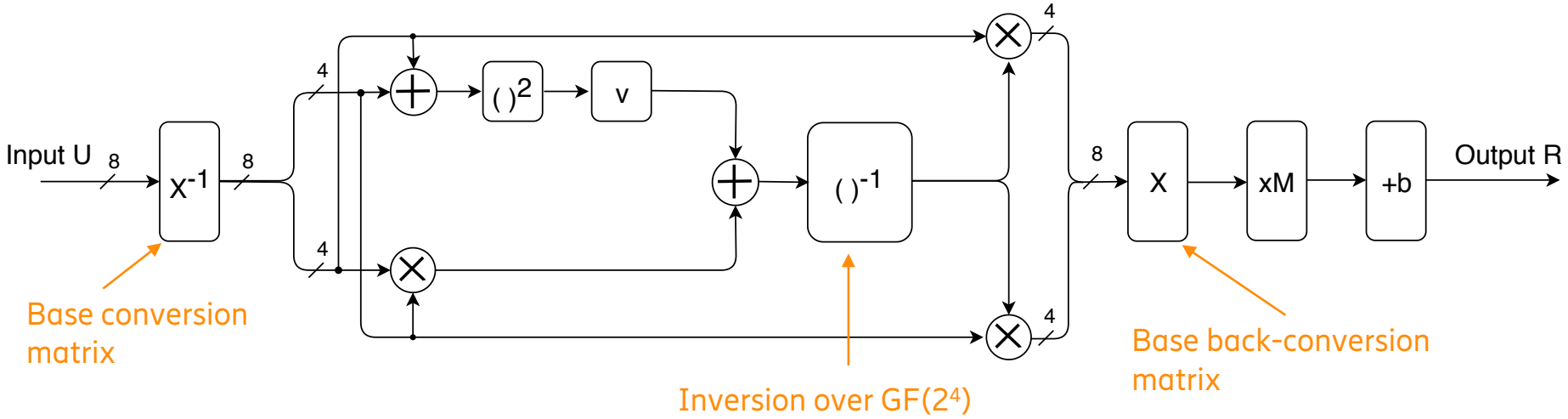
Basic flow of AES SBox



Direct implementation of inversion over Rijndael field is very complex.

Previous work (low area)

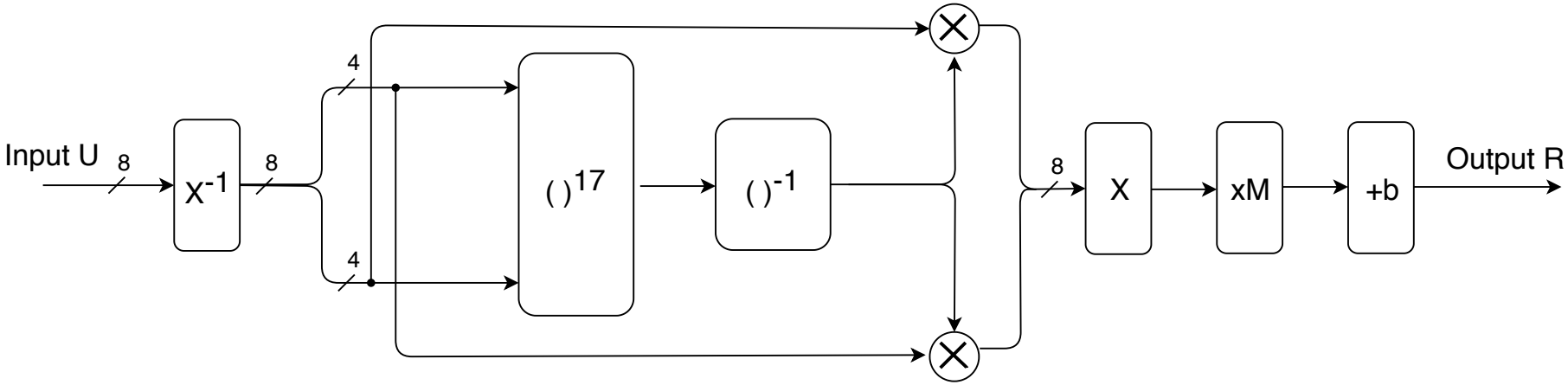
Rijmen [Rij00] proposed (based on Itoh and Tsujii [IT88]) to use a composite field and do the inversion in GF(2^4) instead.



— Satoh et al [SMT01] reduced inversion to GF(2^2).
— Canright [Can05] investigated the importance of subfield representation.

Previous work (low depth)

Boyar, Peralta et al ([BP10a,BP10b,BP12,BFP18]) used a normal base $A=a_0Y + a_1Y^{16}$ and $A^{-1} = (AA^{16})^{-1}A^{16}$ (also based on Itoh and Tsujii [IT88]) to derive another implementation.

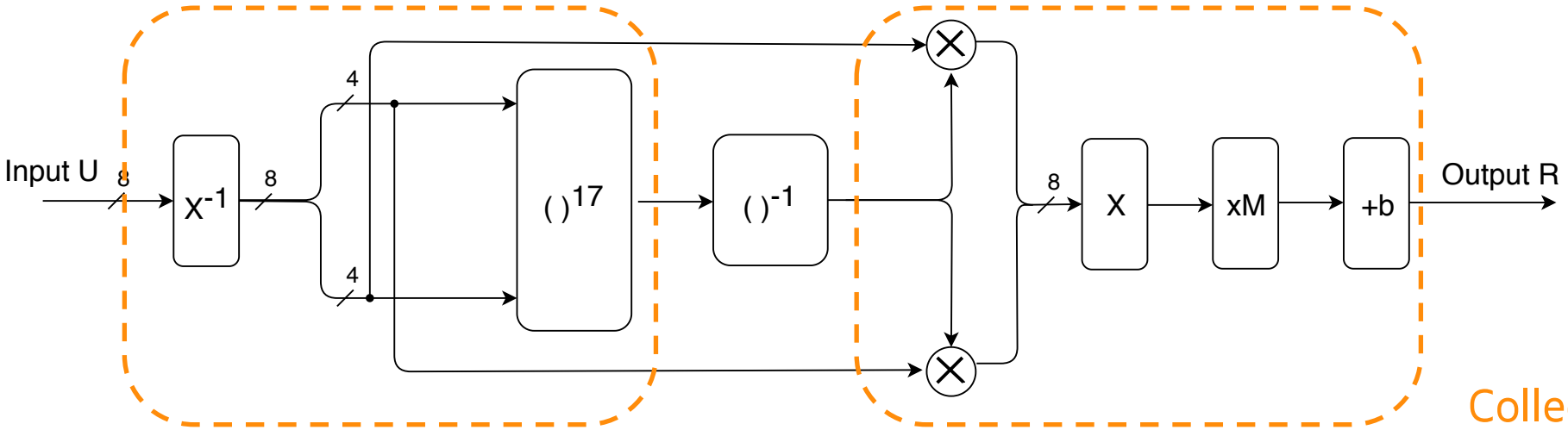


Several papers followed:

— Nogami et al [NNT+10], looking at mixed bases.
— Ueno et al [UHS+15], looking at redundant bases.
— Reyhani et al [RMTA18a,b], improving Boyar-Peralta (BP) search algorithm.
— Li et al [LSL+19], incorporating depth into BP algorithm.

Previous work (low depth)

Boyar, Peralta et al ([BP10a,BP10b,BP12,BFP18]) used a normal base $A=a_0Y + a_1Y^{16}$ and $A^{-1} = (AA^{16})^{-1}A^{16}$ (also based on Itoh and Tsujii [IT88]) to derive another implementation.



Collect all linear terms and push into two matrices.

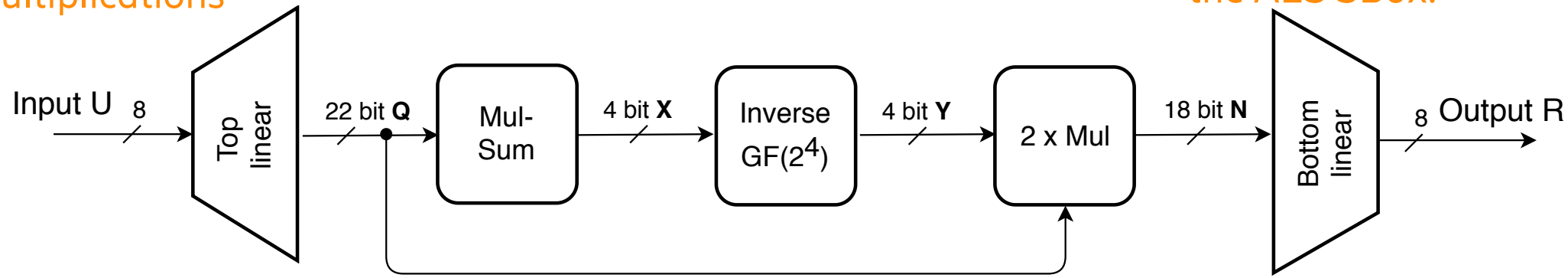
Several papers followed:

— Nogami et al [NNT+10], looking at mixed bases.
— Ueno et al [UHS+15], looking at redundant bases.
— Reyhani et al [RMTA18a,b], improving Boyar-Peralta (BP) search algorithm.
— Li et al [LSL+19], incorporating depth into BP algorithm.

Architectural starting point [BP12]

Base conversion and generation of linear parts of multiplications

Base back-conversion and the affine transformation of the AES SBox.



Basic problem statement:

Given a binary matrix M_{mxn} and the maximum allowed depth maxD, find the circuit of depth D ≤ maxD with the minimum number of 2-input XOR gates such that it computes $Y = M \cdot X$.

$$\begin{aligned} y_0 &= x_0 + x_2 + x_3 + x_4 \\ y_1 &= x_1 + x_2 + x_4 \\ y_2 &= x_0 + x_1 + x_3 + x_4 \end{aligned} \qquad M = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Additional Input Requirement (AIR)

- Input signals may arrive with different delay d_i

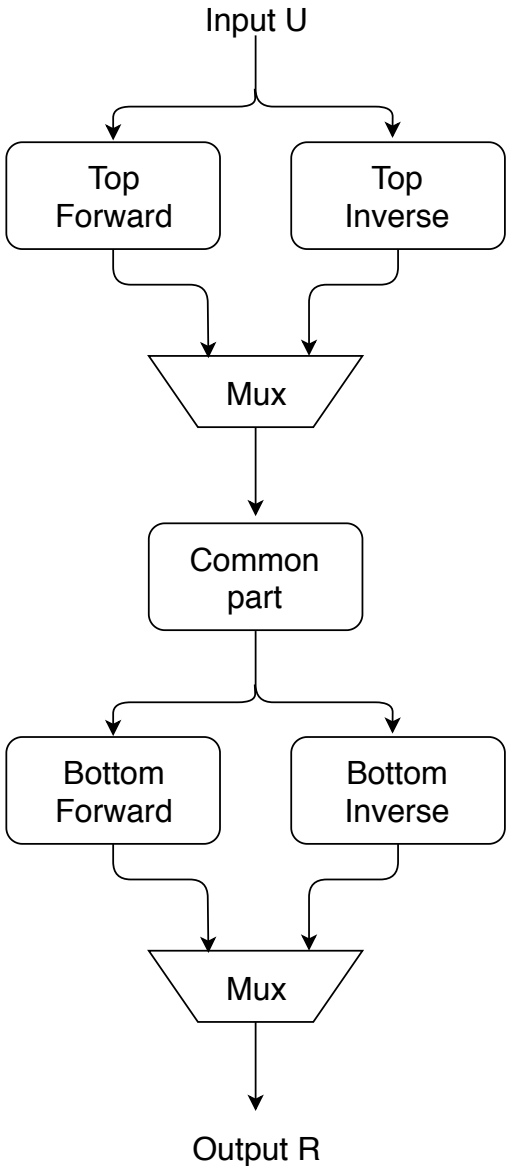
Additional Output Requirement (AOR)

- Output signals may need to be ready earlier, $e_i \leq maxD$

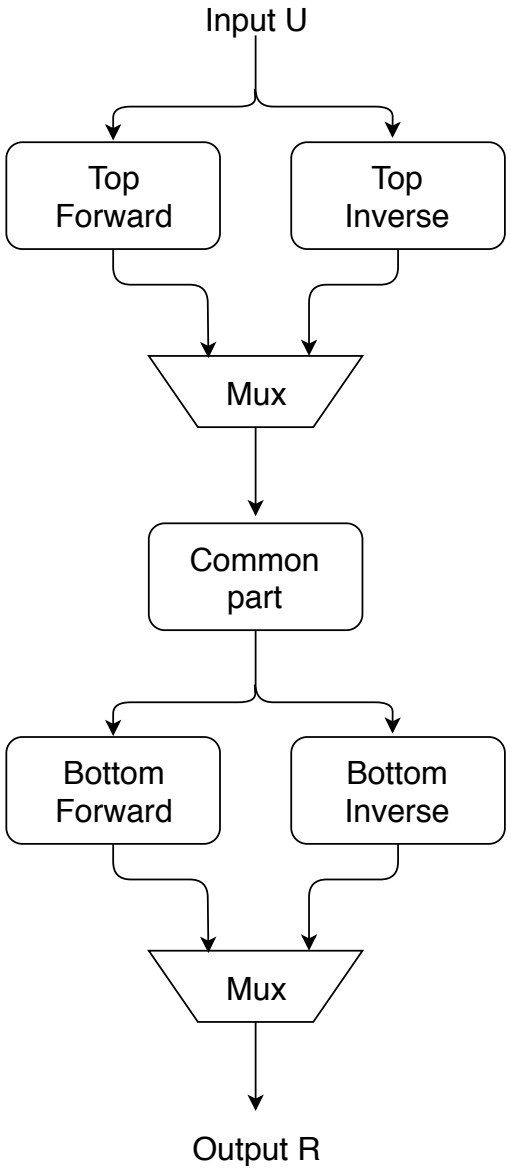
Our contributions

- New techniques for minimizing the Top and Bottom matrices (area with delay constraints).
  - Introduced a probabilistic heuristic approach to the cancellation-free algorithm by Paar [Paa97].
  - New cancellation-allowed exhaustive search algorithm, based on BP-algorithm [BP10a].
- Floating Multiplexers for the combined SBox.
- New generalization of BP-algorithm, allowing other types of gates.
  - New metrics, with lots of speed up tricks for the distance function.
  - Stack algorithm with a search tree.
- New architecture that removes the Bottom matrix and reduces the overall depth.
- New circuit for the inverse operation.
- Additional Transformation Matrices.

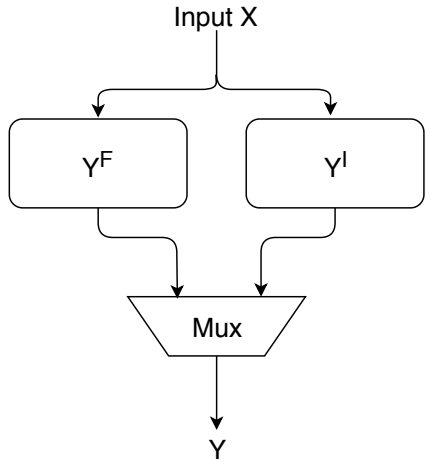
Combined SBox with multiplexers



Combined SBox with multiplexers



Example:



$$Y^F = X_0 + X_1$$
$$Y^I = X_0 + X_2$$
$$Y = \mathrm{MUX}(\mathrm{select}, X_0 + X_1, X_0 + X_2)$$

Replace with:

$$Y = \mathrm{MUX}(\mathrm{select}, X_1, X_2) + X_0$$

Generally:

$$Y = \mathrm{A} + \mathrm{MUX}(\mathrm{select}, B, C) \rightarrow$$
$$Y = \mathrm{A} + \Delta + \mathrm{MUX}(\mathrm{select}, \mathrm{B} + \Delta, C + \Delta)$$

Boyar-Peralta algorithm [BP10a]

— Notion of a "**point**".
  — In original algorithm, this is a linear combination of input signals. Set of gates used G ={XOR}.

— Base set of **known** points S.

$$S_0 = (x_0, x_1, \dots, x_4) = ([1,0,0,0,0], [0,1,0,0,0], \dots, [0,0,0,0,1])$$

— Set of **target** points T, the rows y_i of M.

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}$$

— **Metric** using a distance function $\delta_i(S, y_i)$.

$$\Delta = (\delta_0, \delta_1, \dots, \delta_{n-1}).$$

— Set of **candidates** C.

- Try all base pair s_i, s_j in S_t and form a candidate $c = g(s_i, s_j)$, in this case: $c = s_i + s_j$
- Calculate the new distance vector Δ based on $S_t \cup c$
- We save the candidate c that gives the lowest distance $S_{t+1} = S_t \cup c$
- Repeat until the distance vector is all-zero.

BP for Linear Circuits with Floating Multiplexers

- Include MUX, NMUX in the set of gates.

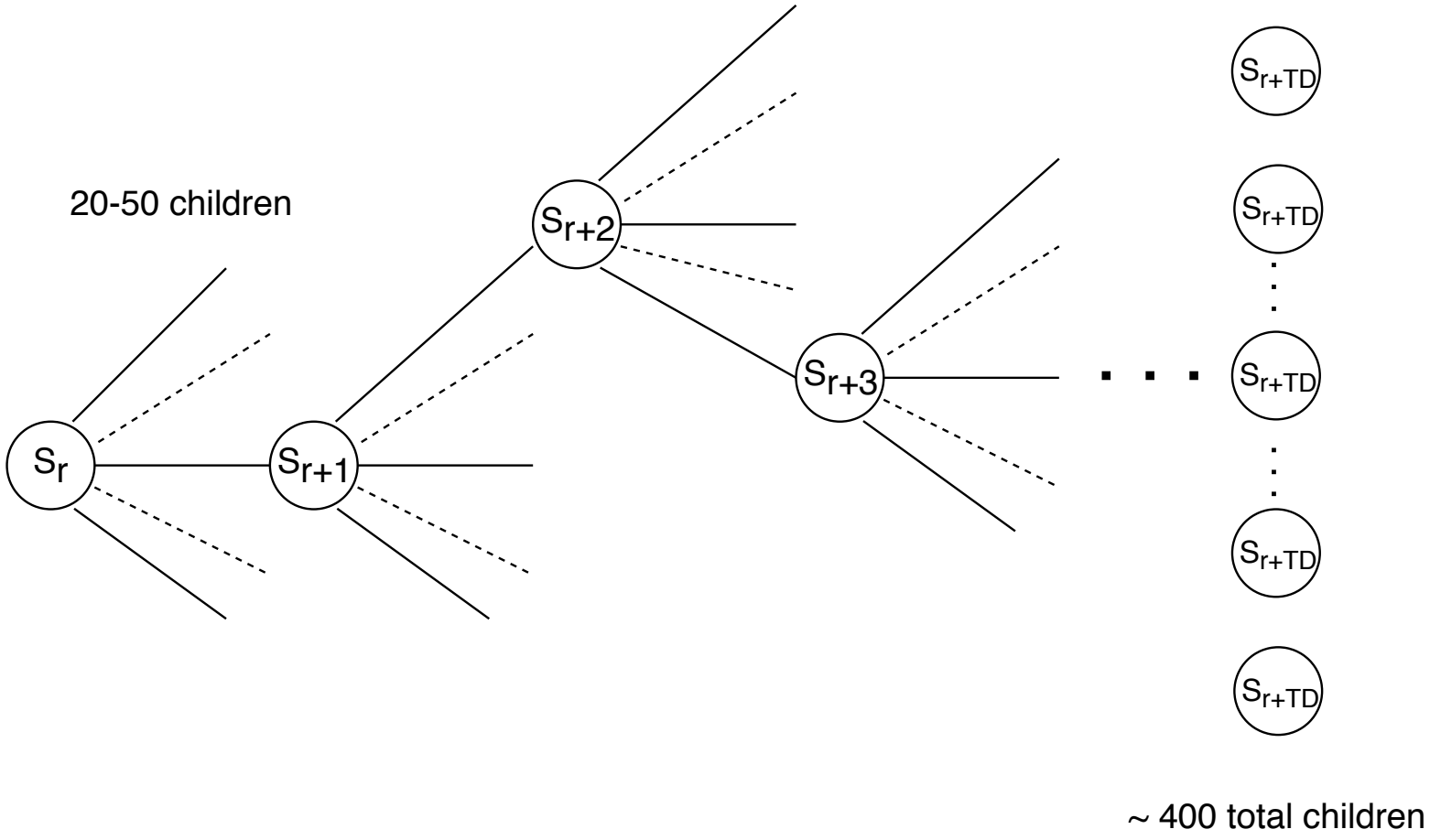
The six gates	
MUX(v,w)	MUX(w,v)
NMUX(v,w)	NMUX(w,v)
XOR(v,w)	XNOR(v,w)

- A **point** is now a tuple $p = (F, I)$
  - F and I are linear combinations of input signals
  - Translated into $MUX(ZF, F \cdot X, I \cdot X)$
- Input points $X_k = \left(2^k, 2^k\right), k = 0, \ldots n-1$
- Target points $Y_k = \left(Y_k^F, Y_k^I\right), k = 0, \ldots, m-1$
- Improved metrics and new algorithm (with lots of speed up) to calculate $\delta_i(S, y_i | Dmax)$.
- We keep track of AIR, and AOR at each stage.
- For the full Affine transformation, define the point as $p = (f, F, i, I)$ → $MUX(ZF, F \cdot X + f, I \cdot X + i)$

BP for any Nonlinear Circuit

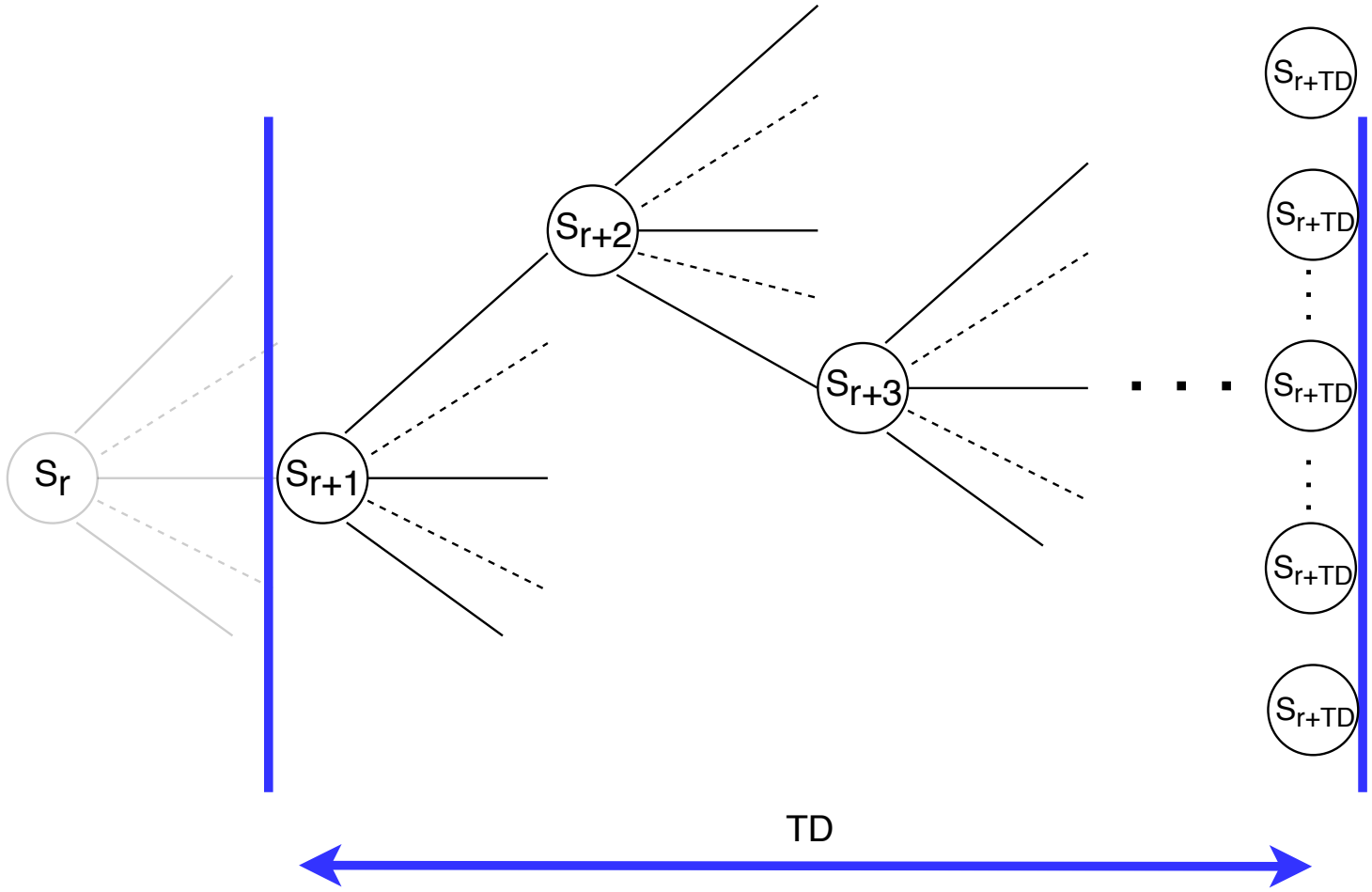
- Allow all kinds of gates in G (XOR, AND, MUX, … 2-input, 3-input…).
- A **point** is now the truth table of a Boolean function.
  - Combine points using truth tables and gate functionality.
- **Target** points are the truth table for every output signal of the nonlinear block.
- Applicable to circuits of maximum 4-5 input signals, and the number of output signals is not limited.
- Used to derive a smaller inversion circuit over GF(2^4).

Search Tree



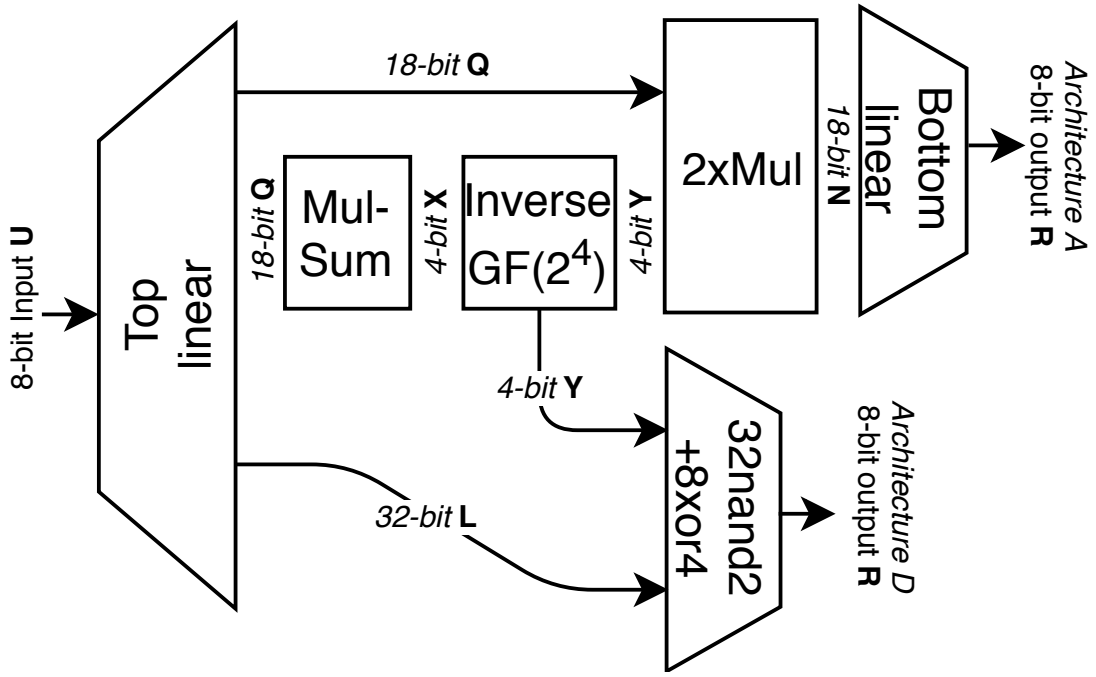
— Try to keep leaves from as many different branches as possible

Search Tree



— Try to keep leaves from as many different branches as possible

New architecture for lower depths



The Bottom matrix only depends on the multiplication of the 4-bit signal **Y** with some linear combination of the input signal **U**

$$\boldsymbol{R} = Y_0 \cdot M_0 \cdot \boldsymbol{U} + \cdots + Y_3 \cdot M_3 \cdot \boldsymbol{U}$$

where M_i is an 8x8 matrix to be scalar multiplied by the Y_i bit.

Calculate M_i in parallel in Top matrix.

Assembling requires 56 gates (32NAND, 24XOR)

New circuit for the inversion in GF(2^4)

$$
\begin{aligned}
Y_0 &= X_1X_2X_3 + X_0X_2 + X_1X_2 + X_2 + X_3 \\
Y_1 &= X_0X_2X_3 + X_0X_2 + X_1X_2 + X_1X_3 + X_3 \\
Y_2 &= X_0X_1X_3 + X_0X_2 + X_0X_3 + X_0 + X_1 \\
Y_3 &= X_0X_1X_2 + X_0X_2 + X_0X_3 + X_1X_3 + X_1
\end{aligned}
$$

- In [BP12] they found a circuit of 17 gates and depth 4 (with base gates {AND, XOR}).
- By applying the BP-algorithm for general non-linear circuits, we managed to achieve 9 gates and depth 3.

```
T0 = NAND(X0, X2)
T1 = NOR(X1, X3)
T2 = XNOR(T0, T1)
T3 = MUX(X1, X2, 1)
T4 = MUX(X3, X0, 1)
Y0 = MUX(X2, T2, X3)
Y1 = MUX(T2, X3, T3)
Y2 = MUX(X0, T2, X1)
Y3 = MUX(T2, X1, T4)
```

We also found a small conventional (no MUXes) circuit of 15 gates and depth 3.

Additional Transformation Matrices

Excluding the final constant from the affine transformation, we can write the SBox as:

$$SBox(x) = x^{-1} \cdot A_{8x8}$$

In any field of characteristic 2, squaring, square root, and multiplication by a constant are linear functions. Thus, for any choice of $\alpha = 1 \ldots 255$, and $\beta = 0 \ldots 7$ we have:

$$Z(x) = \left(\alpha \cdot x^{2^\beta}\right)^{-1}$$ Top matrix

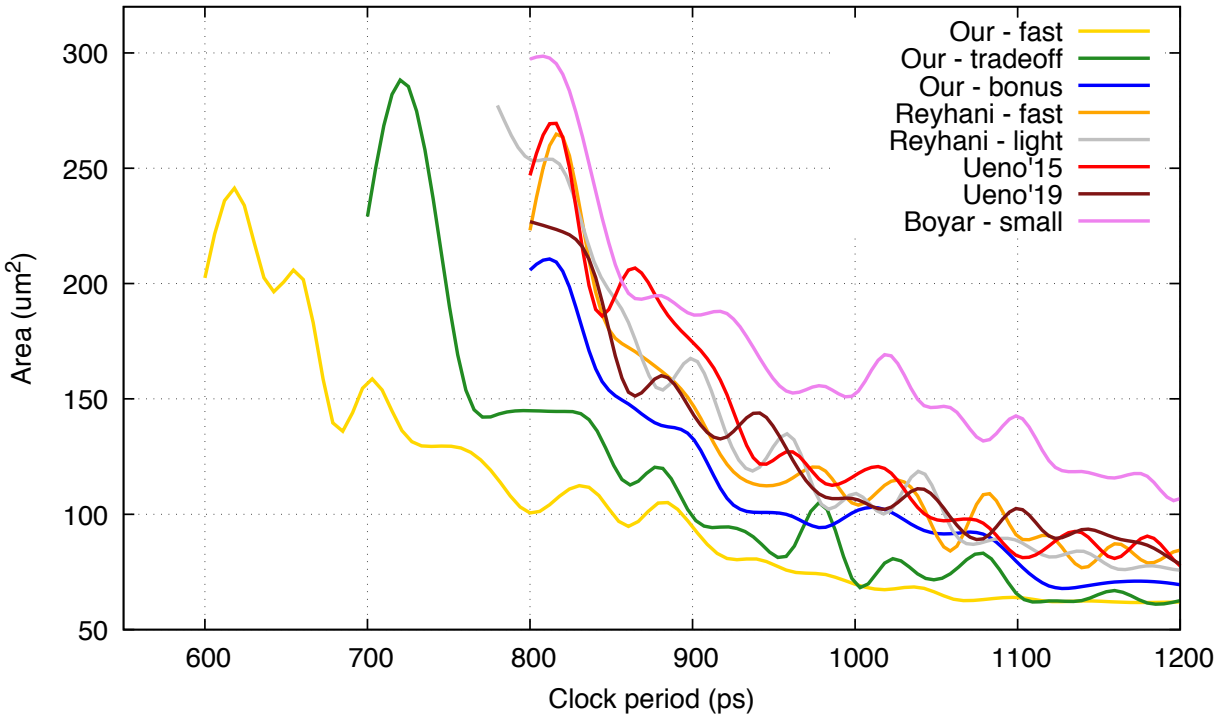
$$SBox(x) = \sqrt[2^\beta]{\alpha \cdot Z(x)} \cdot A_{8x8}$$ Bottom matrix

- For Forward (Inverse) we have 2040 choices. Tried all!
- For Combined we have 2040^2 = 4,161,600 choices. Based on the heuristic algorithm, we selected candidates to run the full generic floating multiplexer algorithm.

A similar approach was independently proposed in [UHNA19] but they only considered multiplication.

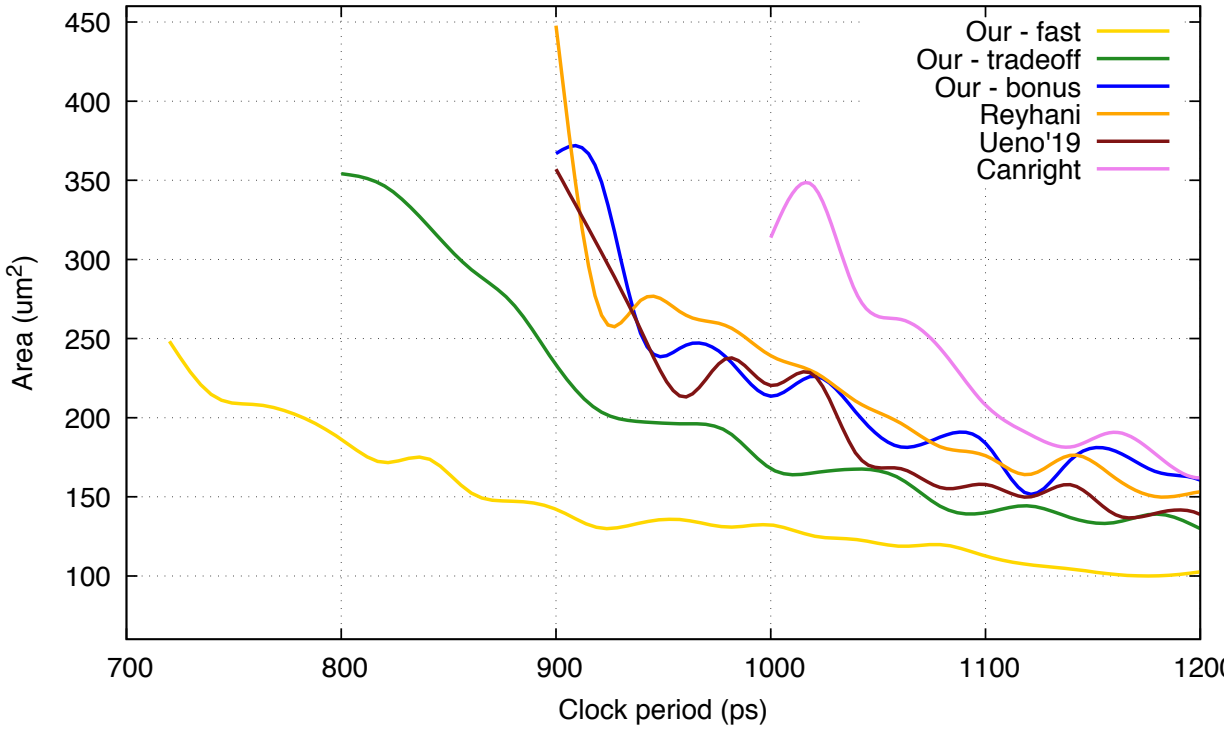
Forward SBox Results

Forward SBox	Area Size/Gates		Critical Path/Depth	
	Std. gates	Tech. GE	Std. gates	Tech. XORs
Previous Results				
Canright [Can05]	80XO+34ND+6NR		19XO+3ND+1NR	
most famous design	120	226.40	23	20.796
Boyar et al [BP12]	94XO+34AD		13XO+3AD	
our starting point	128	264.24	16	14.932
Boyar et al [Boy]	81XO+32ND		21XO+6ND	
record smallest	113	220.73	27	23.508
Ueno et al [UHS+15]	91XO+48ND+13NR (+4IV)		10XO+5ND (+1IV)	
record fastest, formulas from [RMTA18a]	151(+4)	270.71	15(+1)	12.449
Reyhani-Light [RMTA18a]	69XO+43ND+7NR (+4IV)		16XO+4ND (+1IV)	
at CHES 2018	119(+4)	213.45	20(+1)	18.031
Reyhani-Fast [RMTA18a]	79XO+43ND+7NR (+4IV)		11XO+5ND (+1IV)	
at CHES 2018	129(+4)	236.75	16(+1)	13.449
Ueno et al [UHNA19]	90XO+4XN+10OR+45AD (+10IV)		11XO+1OR+3AD (+1IV)	
recent result	149(+10)	298.87	15(+1)	14.131
Our Results				
Forward (fast)	77XO+1XN+4AD+37ND+5NR+6MX		7XO+1XN+1AD+2NR+1MX	
fast with depth 12	130	243.04	12	10.496
Forward (tradeoff)	61XO+8XN+27ND+5NR+8MX+2MI		8XO+2ND+1ND+2NR+1MX	
area/speed tradeoff	111	216.75	14	12.263
Forward (bonus)	58XO+6XN+27ND+5NR+6MX		18XO+2XN+1ND+2NR+1MX	
new record smallest	102	195.10	24	22.263



Combined SBox Results

Combined SBox	Area Size/Gates		Critical Path/Depth	
	Std. gates	Tech. GE	Std. gates	Tech. XORs
Previous Results				
Canright [Can05]	94XO+34ND+6NR+16MX (+2IV)		20XO+3ND+2OR+5NR	
most famous design	150(+2)	297.64	30	25.644
Reyhani et al [RMTA18b]	81XO+32ND+4OR+16NR+16MI (+8IV)		17XO+2ND+3OR+6NR	
	149(+8)	290.13	28	23.608
Ueno et al [UHNA19]	112XO+7XN+10OR+45AN+16MX (+10IV)		11XO+3AN+1OR+2MX (+1IV)	
recent result	190 (+10)	393.40	17(+1)	15.681
Our Results				
Combined (fast)	77XO+27XN+41ND+6NR+13MX+12MI		6XO+3XN+1ND+2NR+1MX+1MI	
fast with depth 14	176	351.65	14	12.312
Combined (tradeoff)	70XO+21XN+27ND+5NR+17MX+5MI		7XO+4XN+1ND+2NR+1MX+1MI	
area/speed tradeoff	145	296.99	16	14.305
Combined (bonus)	70XO+9XN+27ND+5NR+16MX		15XO+4XN+2ND+1NR+3MX	
new record smallest	127	253.35	25	22.675



AES MixColumns results

Alexander also applied the algorithms to the AES MixColumns circuits

Previous results (XORs):	
103	Jean et al, CHES 2017
97	Krantz et al, ToSC 2017
95	Banik et al, ePrint Archive Report 2019/856
94	Tan and Peyrin, ePrint Archive Report 2019/847
Alexander's result:	
92 (depth 6)	Alexander Maximov, ePrint Archive Report 2019/833

Thank you.

www.ericsson.com