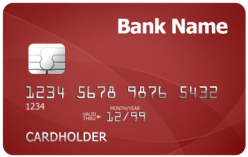
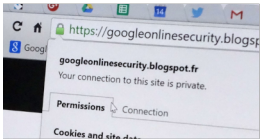
Optimizations in Symmetric Cryptography

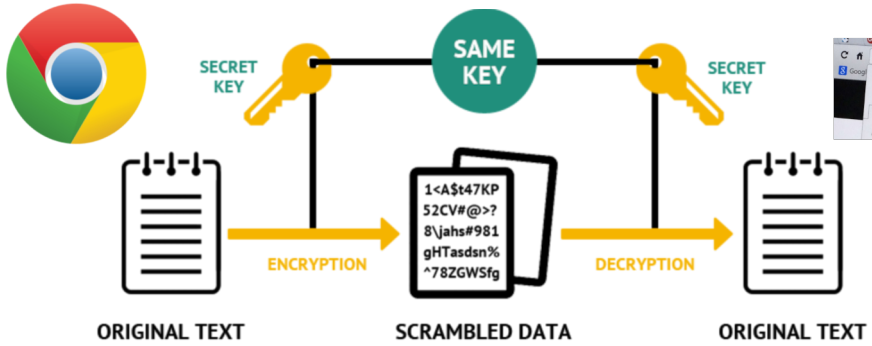
Ko Stoffelen

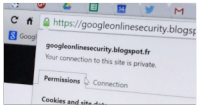
Cryptography





Symmetric Cryptography





Chapter 3: S-boxes

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
y	14	4	11	2	3	8	0	9	1	10	7	15	6	12	5	13

Chapter 3: S-boxes

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
y	14	4	11	2	3	8	0	9	1	10	7	15	6	12	5	13

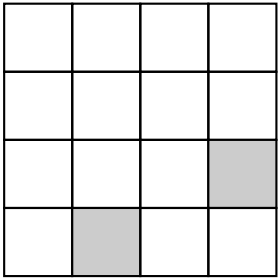
$$t_0 = x_0 \vee x_1$$
$$t_1 = t_0 \oplus x_3$$
$$y_0 = \neg t_1$$
$$t_3 = x_2 \vee y_0$$
$$y_2 = t_3 \oplus x_1$$

$$t_5 = x_1 \vee x_2$$
$$t_6 = t_5 \oplus x_0$$
$$t_7 = t_1 \wedge t_6$$
$$y_3 = x_2 \oplus t_7$$
$$y_1 = \neg t_6$$

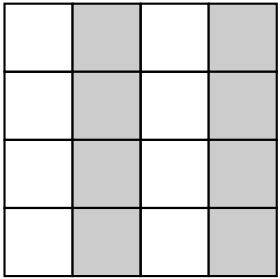
Chapter 4: MDS Matrices

Chapter 4: MDS Matrices

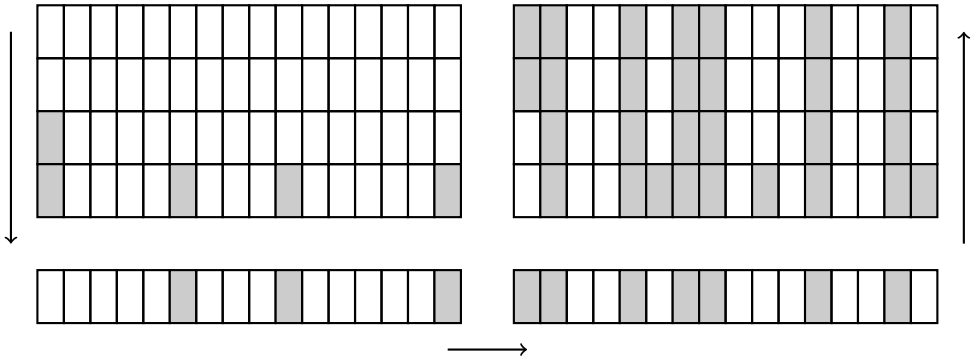
$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}$$



$=$

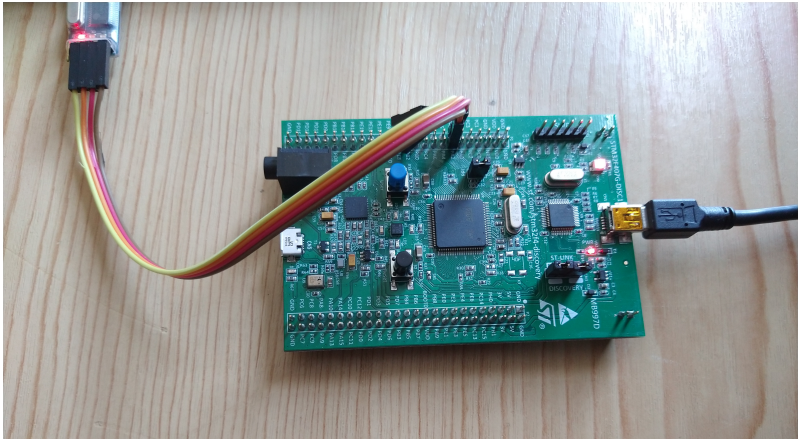


Chapter 5: Column-Parity Mixers

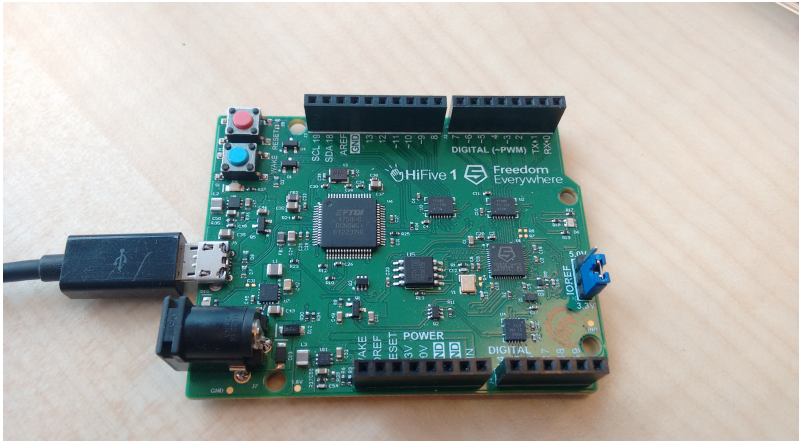


Chapter 6: ARM Cortex-M

Chapter 6: ARM Cortex-M

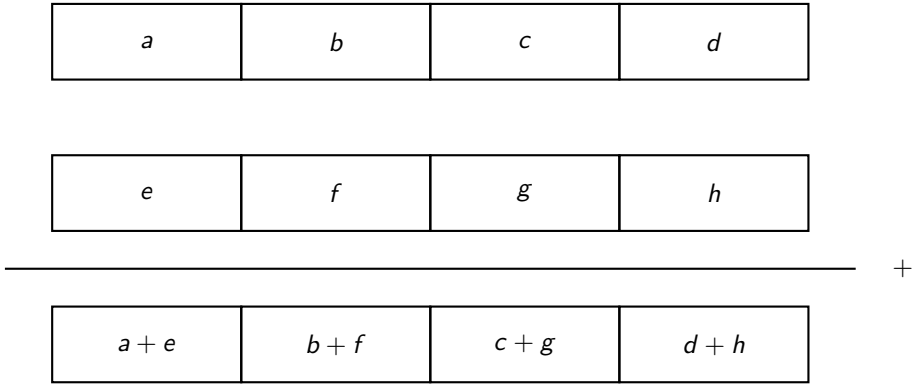


Chapter 7: RISC-V



Chapter 8: Vectorization

Chapter 8: Vectorization



Chapter 9: Reusing Randomness