Symmetrie in de symmetrische cryptografie

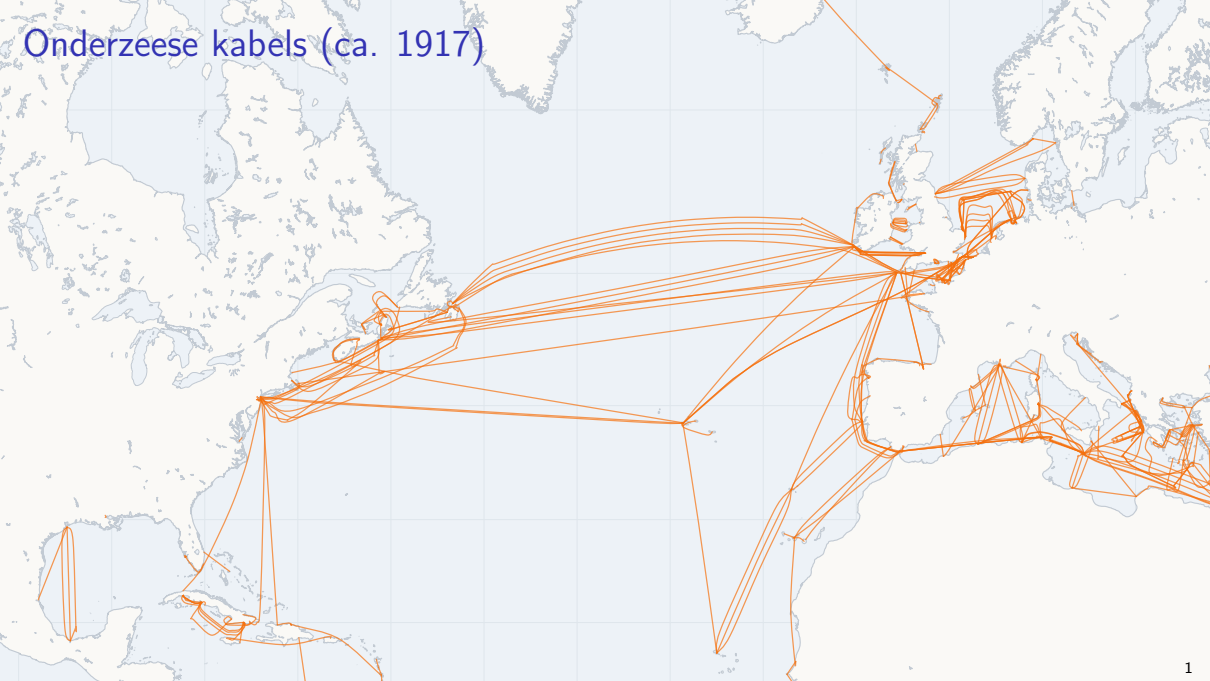
Tim Beyne

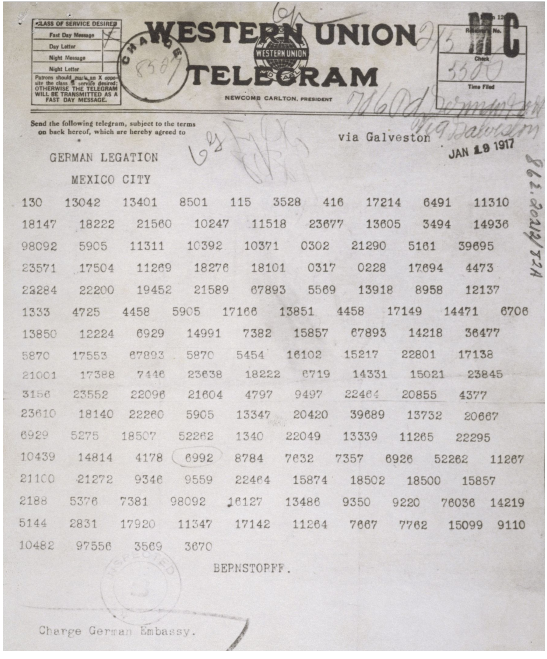
COSIC, KU Leuven

18 september 2026



Onderzeese kabels (ca. 1917)





CLASS OF SERVICE DESIRED
Fast Day Message
Day Letter
Night Message
Night Letter
Patrons should check class of service desired; otherwise the telegram will be transmitted as a fast day message.

CHARGE

WESTERN UNION TELEGRAM

WESTERN UNION

NEWCOMB CARLTON, PRESIDENT

MC

Check

Time Filed

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION

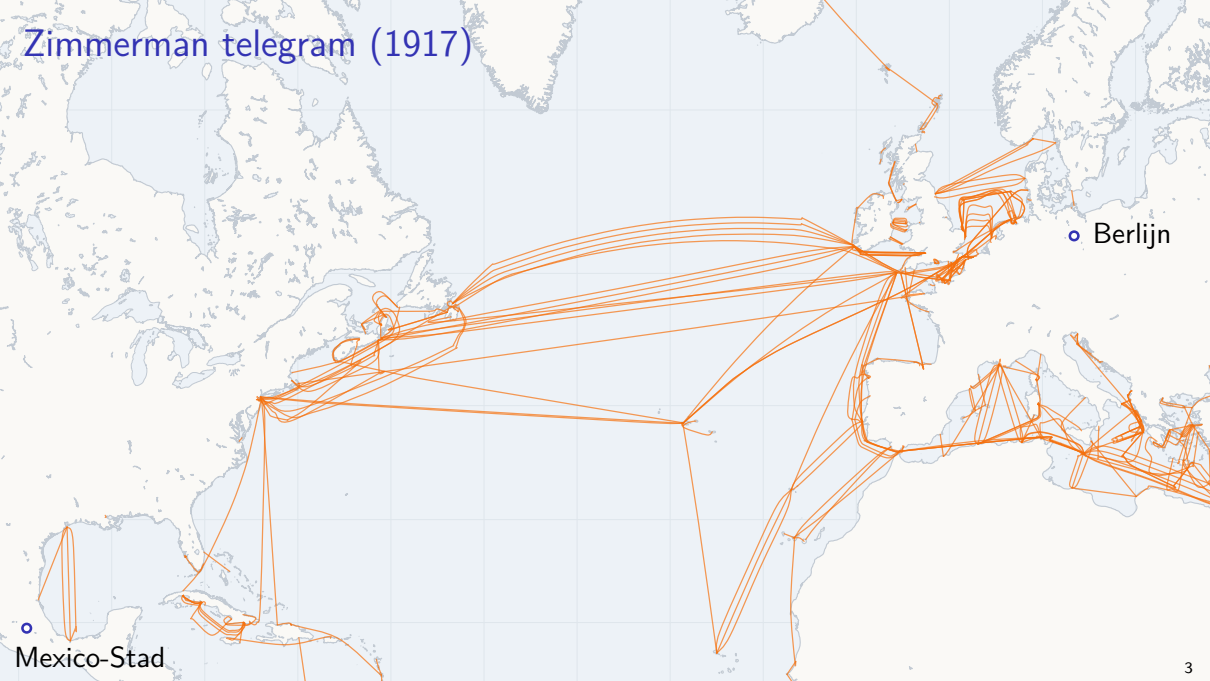
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

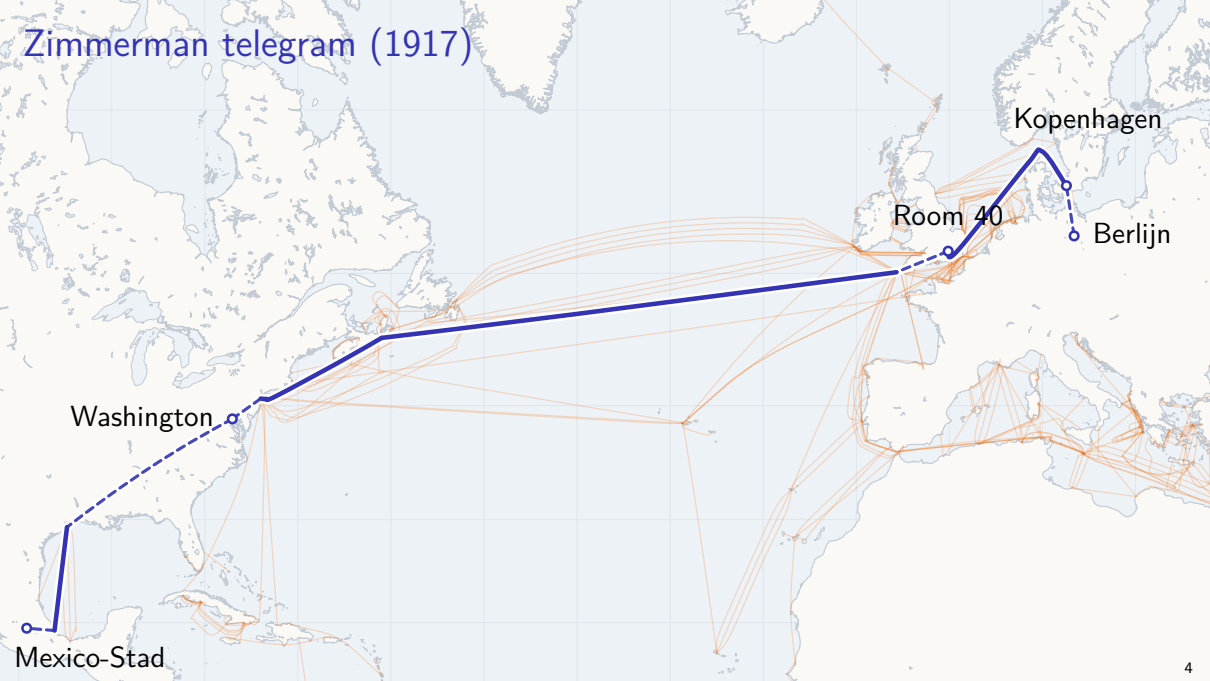
BERNSTORFF.

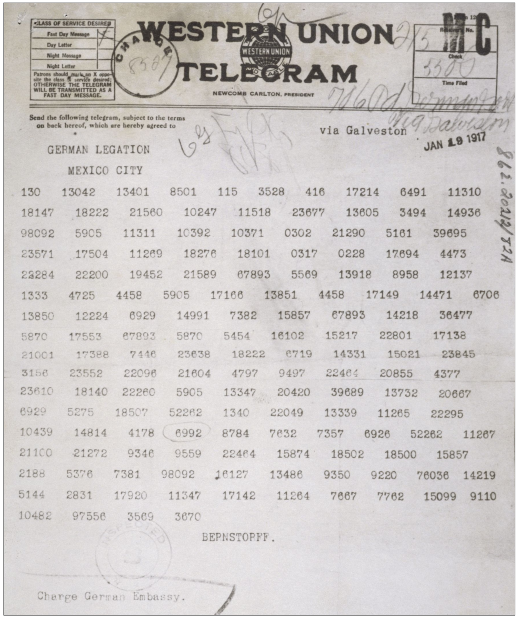
Charge German Embassy.

Zimmerman telegram (1917)



Zimmerman telegram (1917)





•CLASS OF SERVICE DESIRED
Fast Day Message
Day Letter
Night Message
Night Letter
Patrons should check X opposite class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

CHARGE

WESTERN UNION

WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Receiver's No. 135 MC

Check 5350

Time Filed

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 29 1917

GERMAN LEGATION

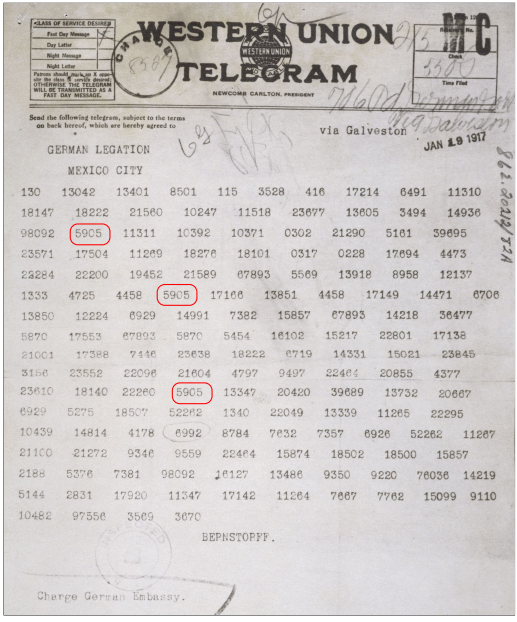
MEXICO CITY

130	13042	13401	8501	115	3528	416	17214	6491	11310	
18147	18222	21560	10247	11518	23677	13605	3494	14936		
98092	5905	11311	10392	10371	0302	21290	5161	39695		
23571	17504	11269	18276	18101	0317	0228	17694	4473		
22284	22200	19452	21589	67893	5569	13918	8958	12137		
1333	4725	4458	5905	17166	13851	4458	17149	14471	6706	
13850	12224	6929	14991	7382	15857	67893	14218	36477		
5870	17553	67893	5870	5454	16102	15217	22801	17138		
21061	17388	7416	23638	18222	6719	14331	15021	23845		
3156	23552	22096	21604	4797	9497	22464	20855	4377		
23610	18140	22260	5905	13347	20420	39689	13732	20667		
6929	5275	18507	52262	1340	22049	13339	11265	22295		
10439	14814	4178	6992	8784	7632	7357	6926	52262	11267	
21100	21272	9340	9559	22464	15874	18502	18500	15857		
2188	5376	7381	98092	16127	13486	9350	9220	76036	14219	
5144	2831	17920	11347	17142	11264	7667	7762	15099	9110	
10482	97556	3569	3670							

BEPNSTORFF.

Charge German Embassy.

21560	- wir
10247	- beabsichtigen
11518	am
23677	ersten
18605	Februar
3494	un.
14963	eingeschränkt
98092	U boot.
5905	Krieg
11311	zu
10392	beginnen
10371	⊙
0302	es ~~twünscht~~ wird
21290	versuchen
5161	werden
39695	V Vereinigten Staaten v. Amerika
23571	trotzdem
17504	neutral



CLASS OF SERVICE DESIRED
Fast Day Message
Day Letter
Night Message
Night Letter
Patrons should check class of service desired; otherwise the telegram will be transmitted as a fast day message.

CHARGE

WESTERN UNION TELEGRAM

WESTERN UNION

NEWCOMB CARLTON, PRESIDENT

Time Filed

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 29 1917

GERMAN LEGATION
MEXICO CITY

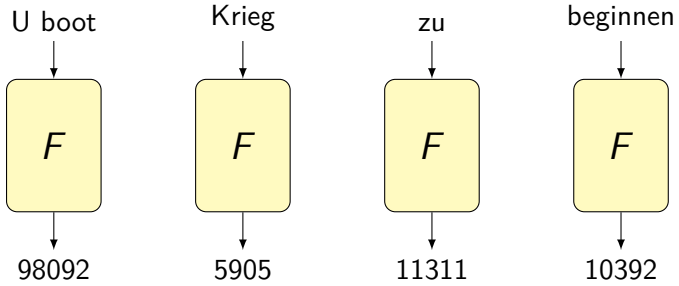
130	13042	13401	8501	115	3528	416	17214	6491	11310
18147	18222	21560	10247	11518	23677	13605	3494	14936	
98092	5905	11311	10392	10371	0302	21290	5161	39695	
23571	17504	11269	18276	18101	0317	0228	17694	4473	
22284	22200	19452	21589	67893	5569	13918	8958	12137	
1333	4725	4458	5905	17166	13851	4458	17149	14471	6706
13850	12224	6929	14991	7382	15857	67893	14218	36477	
5870	17553	67893	5870	5454	16102	15217	22801	17138	
21061	17388	7416	23638	18222	6719	14331	15021	23845	
3156	23552	22096	21604	4797	9497	22464	20855	4377	
23610	18140	22260	5905	13347	20420	39689	13732	20667	
6929	5275	18507	52262	1340	22049	13339	11265	22295	
10439	14814	4178	6992	8784	7632	7357	6926	52262	11267
21100	21272	9340	9559	22464	15874	18502	18500	15857	
2188	5376	7381	98092	16127	13486	9350	9220	76036	14219
5144	2831	17920	11347	17142	11264	7667	7762	15099	9110
10482	97556	3569	3670						

BEPNSTORFF.

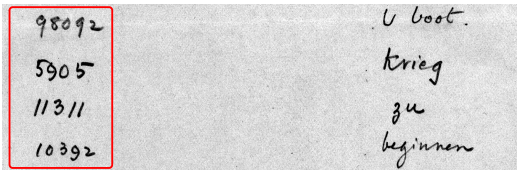
Charge German Embassy.

21560	- wir
10247	- beabsichtigen
11518	am
23677	ersten
18605	Februar
3494	un.
14963	eingeschränkt
98092	U boot.
5905	Krieg
11311	zu
10392	beginnen
10371	⊙
0302	es ~~twünder~~ wird
21290	versuchen
5161	werden
39695	V Vereinigten Staaten v. Amerika
23571	trotz dem
17504	neutral

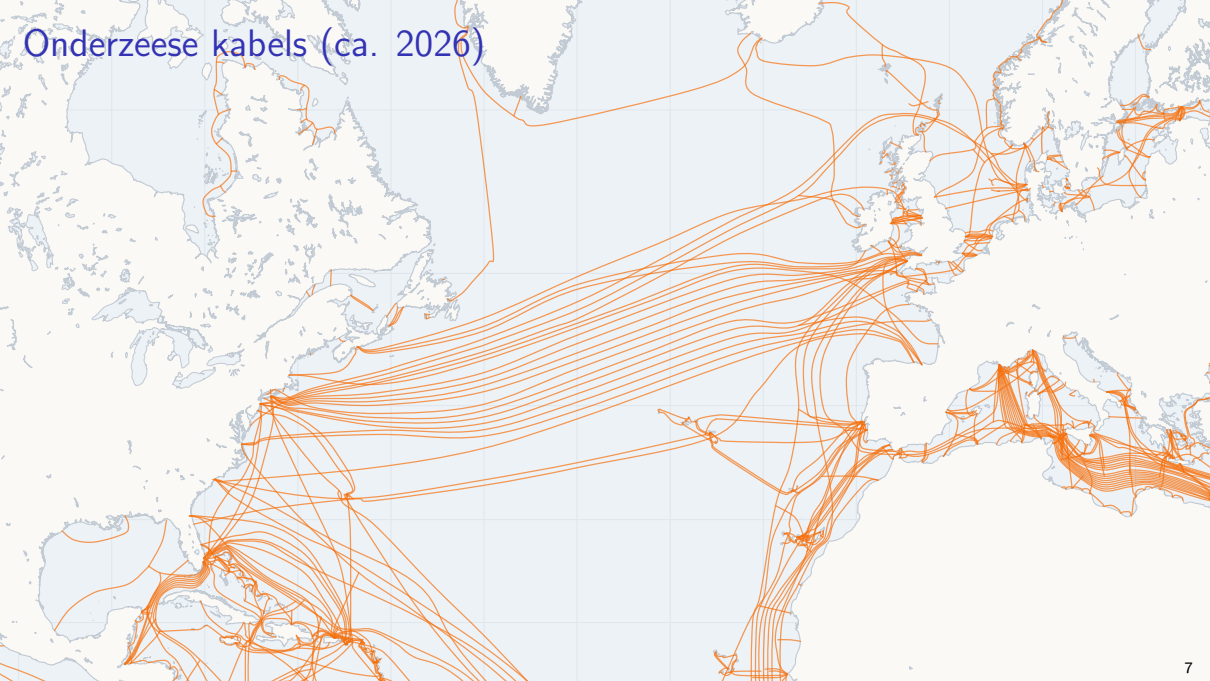
Codeboeken

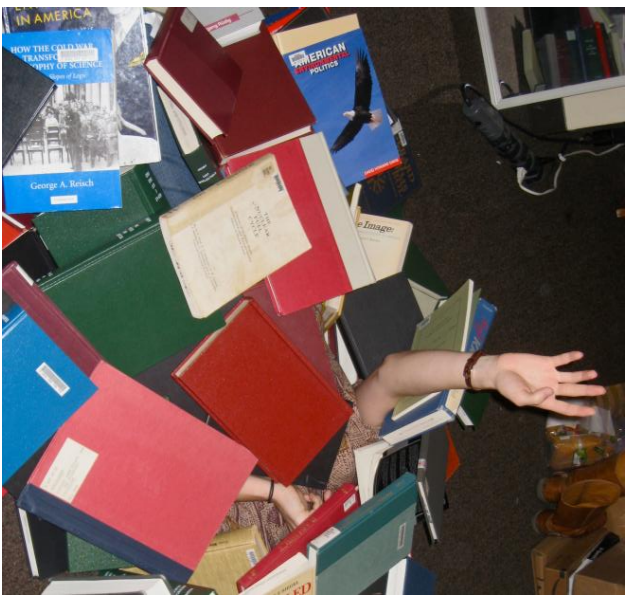


130	13042	13401	8501	115	3528	416
18147	18222	21560	10247	11518	23677	
98092	5905	11311	10392	10371	0302	
23571	17504	11269	18276	18101	0317	
23284	22200	19452	21589	67893	5569	



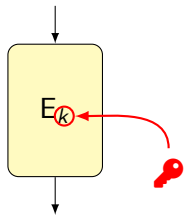
Onderzeese kabels (ca. 2026)




IN AMERICA
George A. Reisch
AMERICAN
POLITICS

Blokcijfers

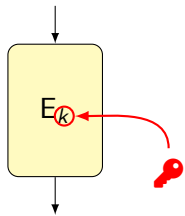
- Moderne cryptografie gebruikt algoritmes in plaats van codeboeken



- Elke sleutel k geeft een nieuw codeboek $E_k : X \to Y$
- Hierdoor kunnen codeboeken veel groter zijn

Blokcijfers

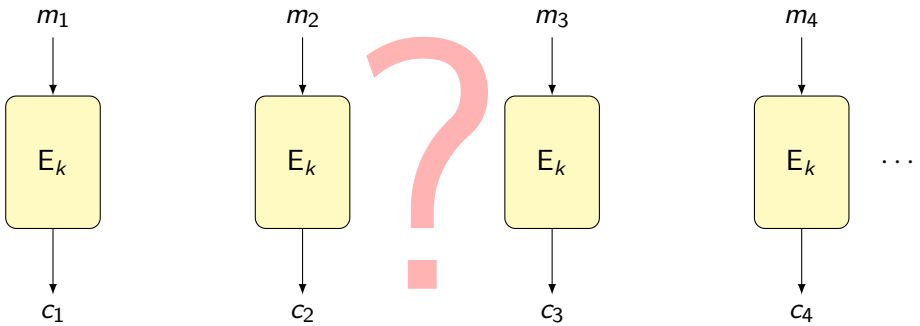
- Moderne cryptografie gebruikt algoritmes in plaats van codeboeken



- Elke sleutel k geeft een nieuw codeboek $E_k : X \to Y$
- Hierdoor kunnen codeboeken veel groter zijn

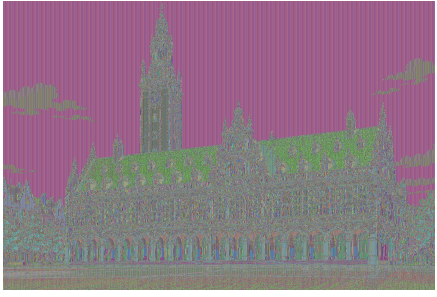
340282366920938463463374607431768211456

Berichten van variabele lengte

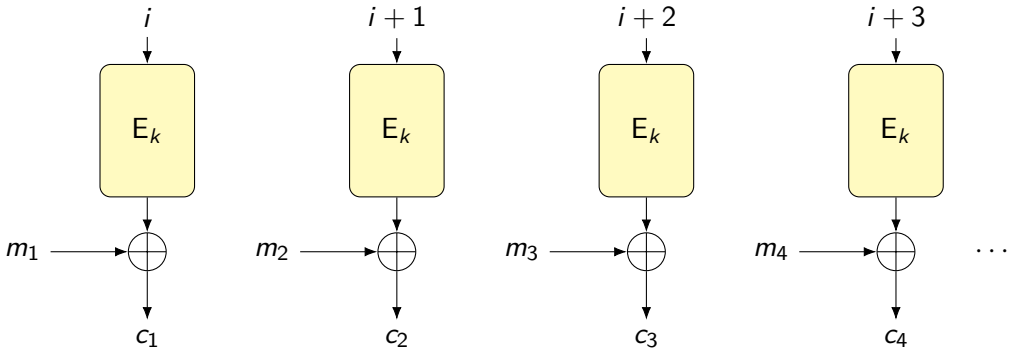


Berichten van variabele lengte



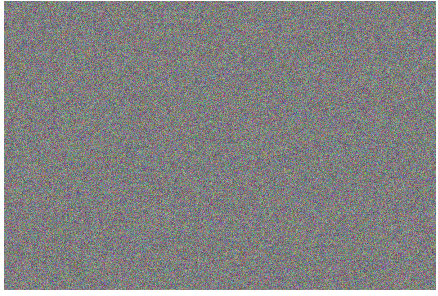


Berichten van variabele lengte



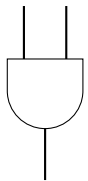
Berichten van variabele lengte



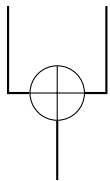


Constructie van blokcijfers

- Samenstelling van eenvoudige operaties, bijvoorbeeld:



en

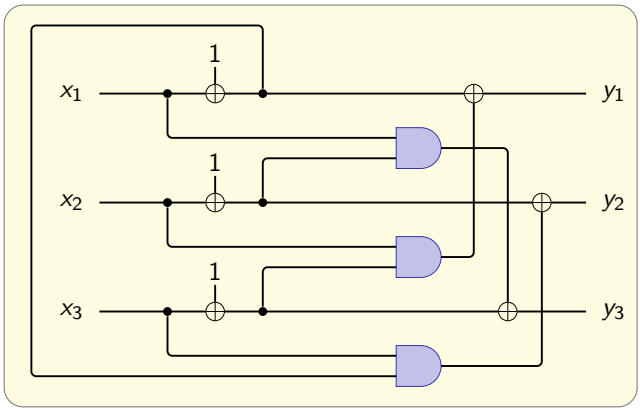


exclusieve of

- $\{0, 1\}$ met deze twee bewerkingen is een veld ($\mathbb{F}_2$)

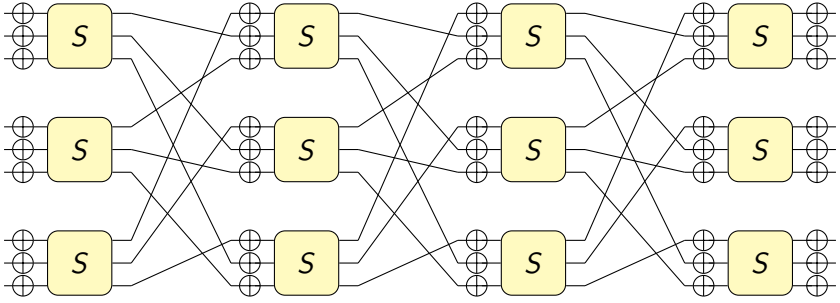
Constructie van blokcijfers

$S\colon \mathbb{F}_2^3 \to \mathbb{F}_2^3$

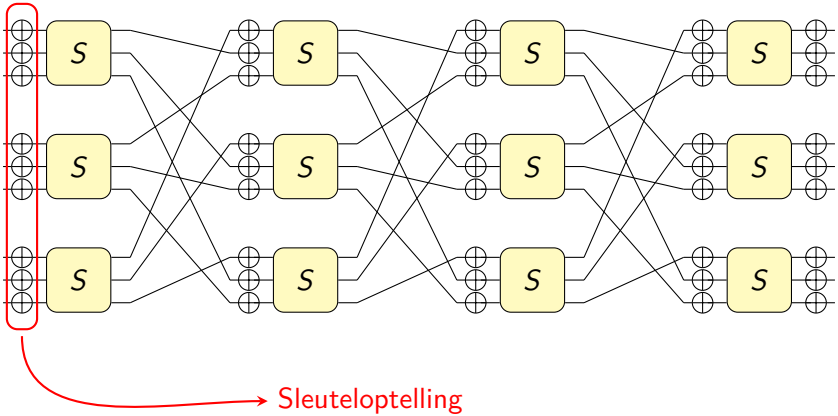


(x_3, x_2, x_1)	000	001	010	011	100	101	110	111
(y_3, y_2, y_1)	111	010	100	101	001	110	011	000

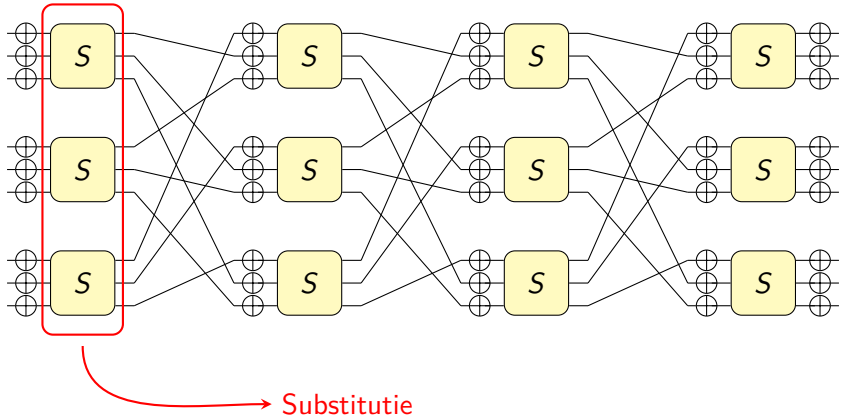
Speelgoedcijfer



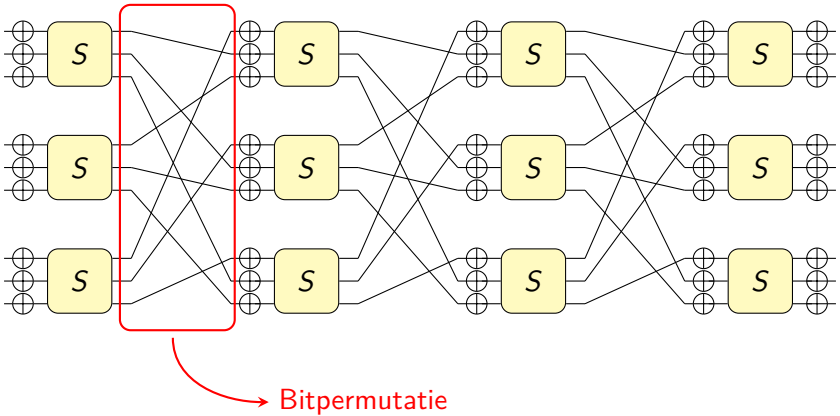
Speelgoedcijfer



Speelgoedcijfer



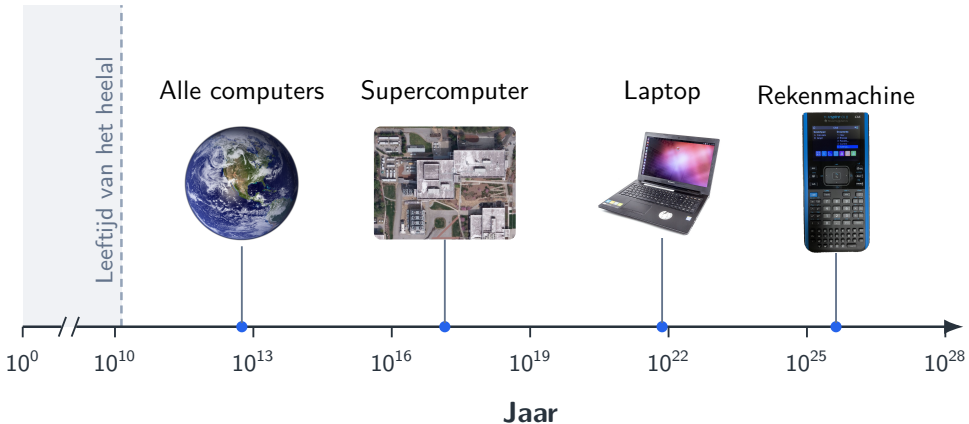
Speelgoedcijfer



Cryptanalyse

Exhaustief zoeken

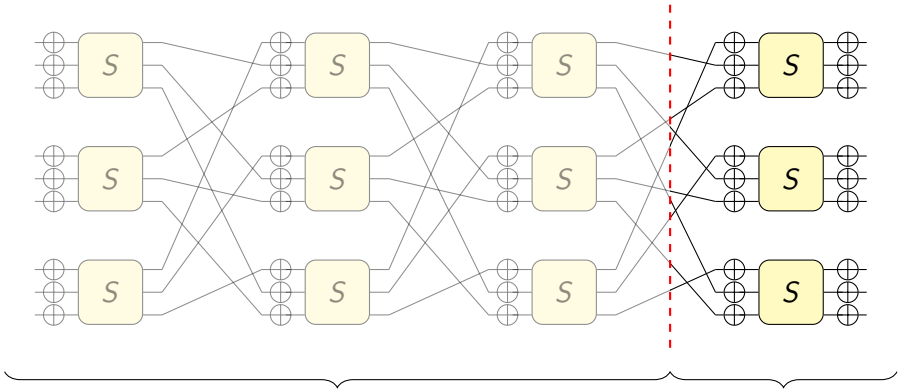
- Probeer alle 2^n sleutels in $\mathbb{F}_2^n$: gemiddeld $2^{n-1} + \frac{1}{2}$ pogingen



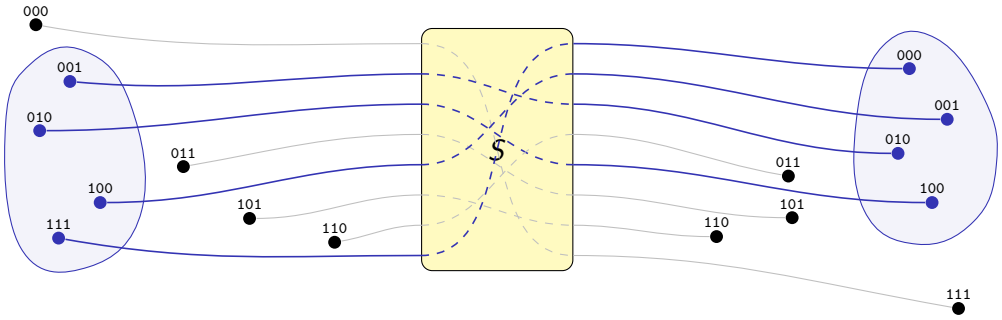
Cryptanalytische aanvallen



Verdeel en heers strategie



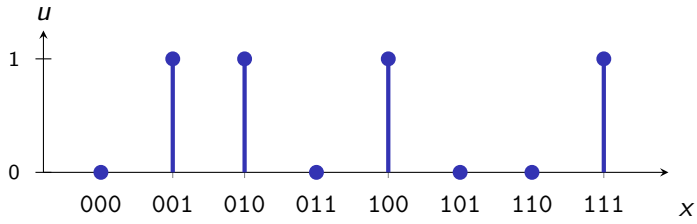
Combinatorische eigenschappen van functies





De vrije vectorruimte

$$\{001, 010, 100, 111\} \subset \mathbb{F}_2^3$$

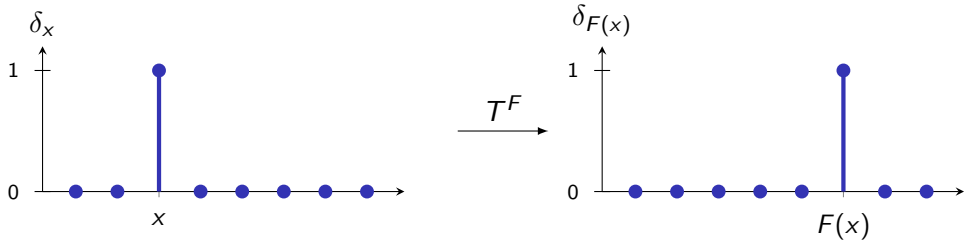


$$u = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$$\mathbb{R}\left[\mathbb{F}_2^3\right]$$

De vrije vectorruimte

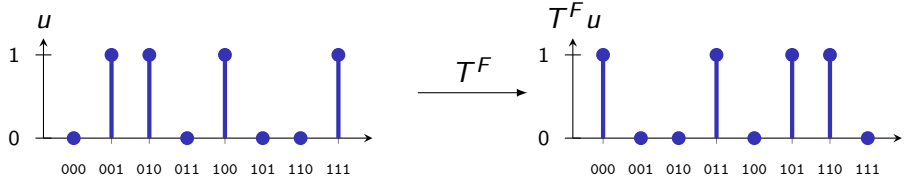
Propagatie voor F



$$T^F = \begin{array}{c} \begin{array}{c} \\ \\ 1 \\ \\ \end{array} \\ \end{array} \begin{array}{c} \overset{x}{\begin{array}{|c|c|c|} \hline & & \\ \hline & & \\ \hline & & \\ \hline \end{array}} \\ \end{array} F(x)$$

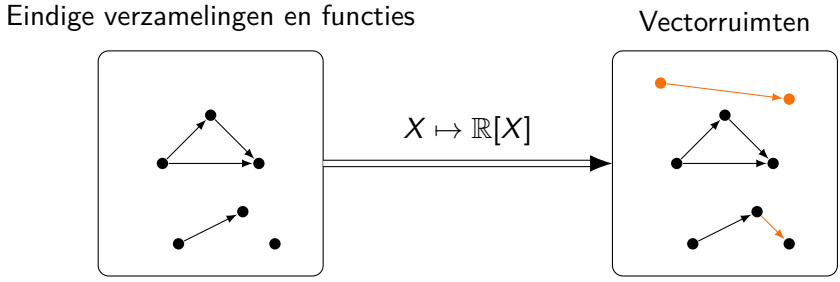
De vrije vectorruimte

Propagatie voor $F(x) = x + 001$

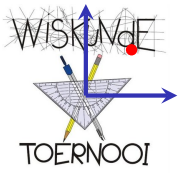


$$T^F u = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

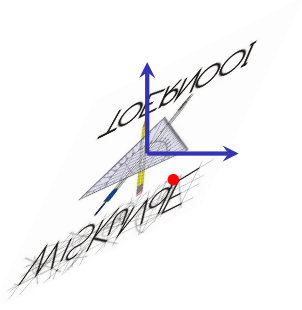
De vrije vectorruimte



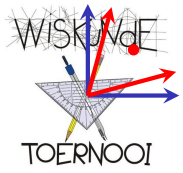
Verandering van basis



$$\begin{bmatrix} 1.15 & -0.58 \\ 0.58 & -1.15 \end{bmatrix}$$

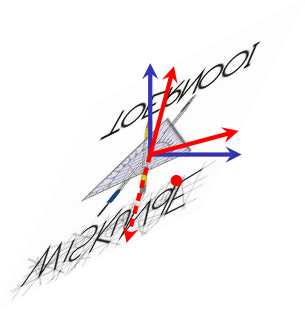


Verandering van basis

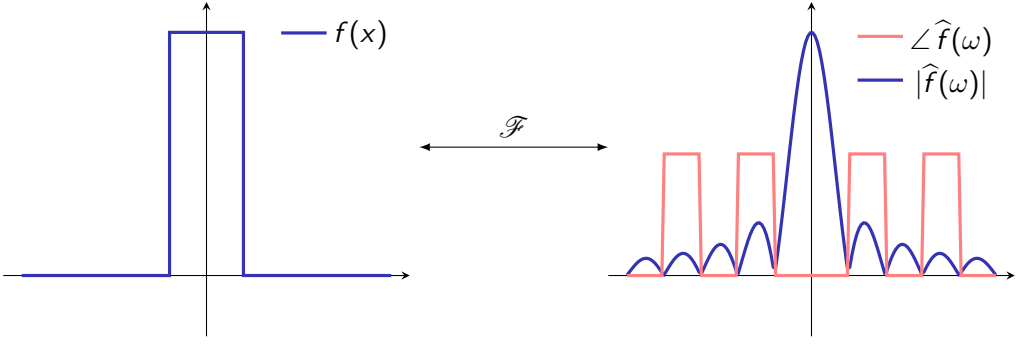


$$\begin{bmatrix} 1.15 & -0.58 \\ 0.58 & -1.15 \end{bmatrix}$$

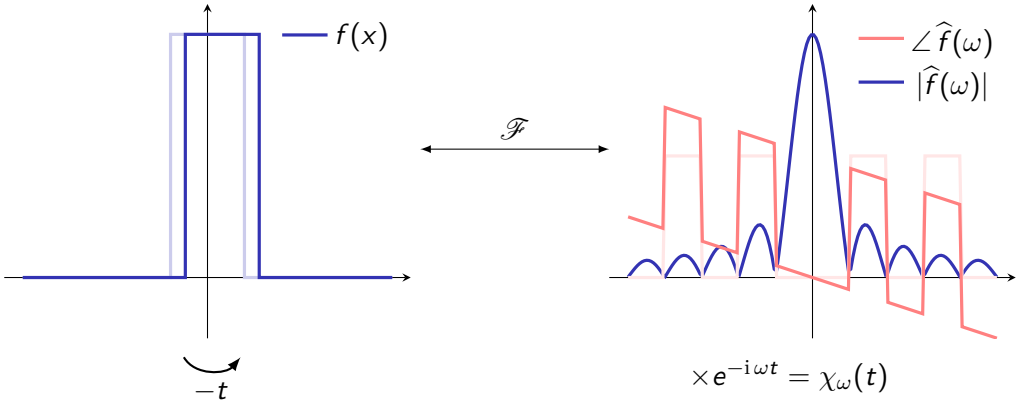
$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



Fourier transformatie



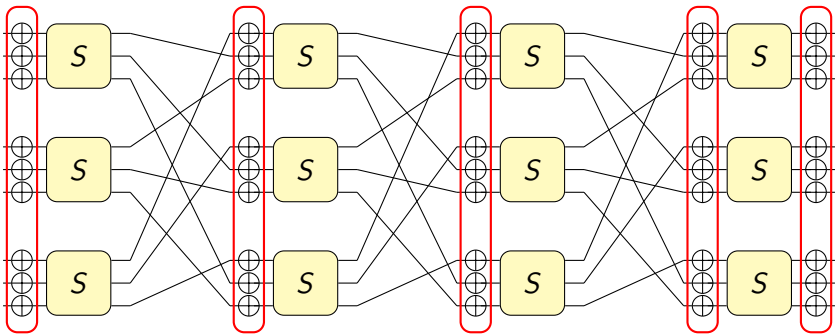
Fourier transformatie



Fourier transformatie diagonaliseert verschuivingen

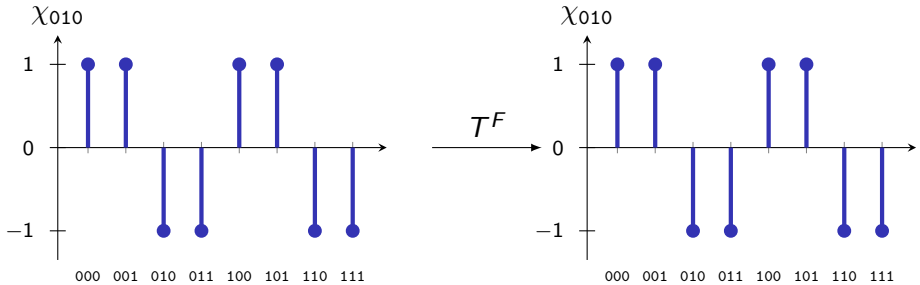
Lineaire cryptanalyse

- $\mathbb{F}_2^n$ is een groep met exclusieve of als optelling



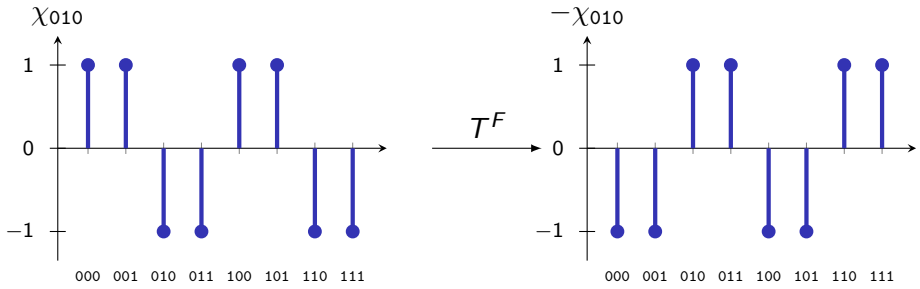
Fourier transformatie op $\mathbb{F}_2^n$

$$F(x) = x + 001$$

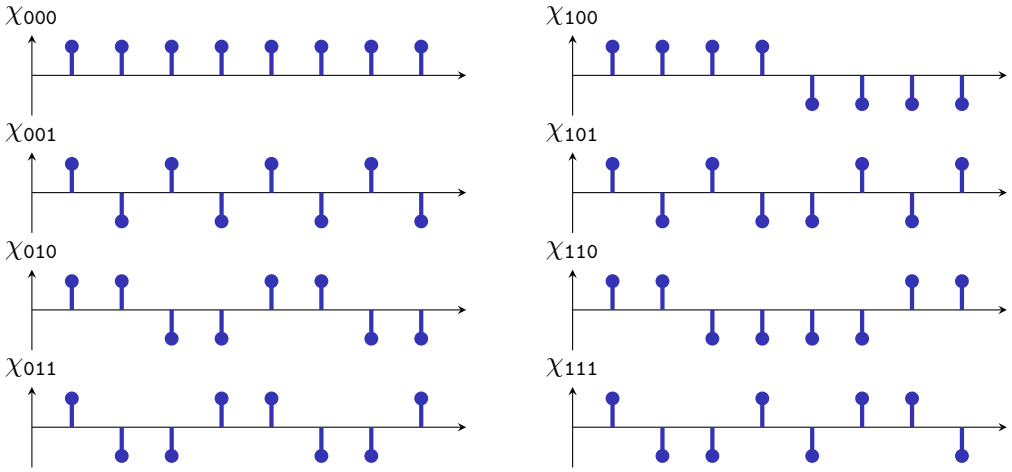


Fourier transformatie op $\mathbb{F}_2^n$

$$F(x) = x + 010$$



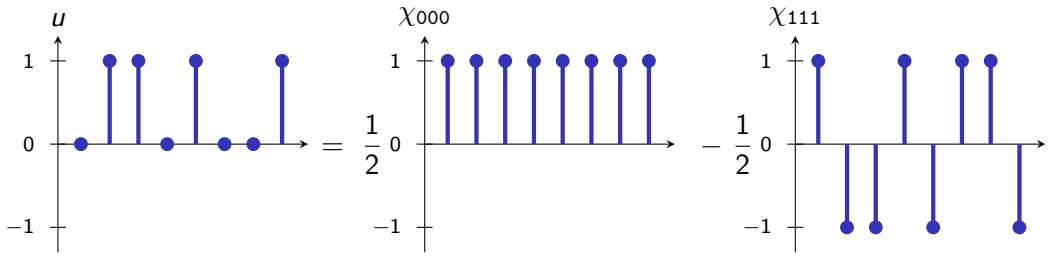
Fourier transformatie op $\mathbb{F}_2^n$



$$\chi_u(x) = (-1)^{u \cdot x} = (-1)^{u_1 x_1 + u_2 x_2 + \cdots + u_n x_n}$$

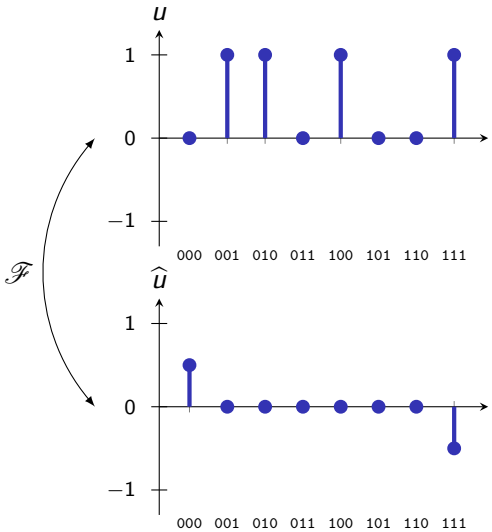
Fourier transformatie op $\mathbb{F}_2^n$

$\{001, 010, 100, 111\}$



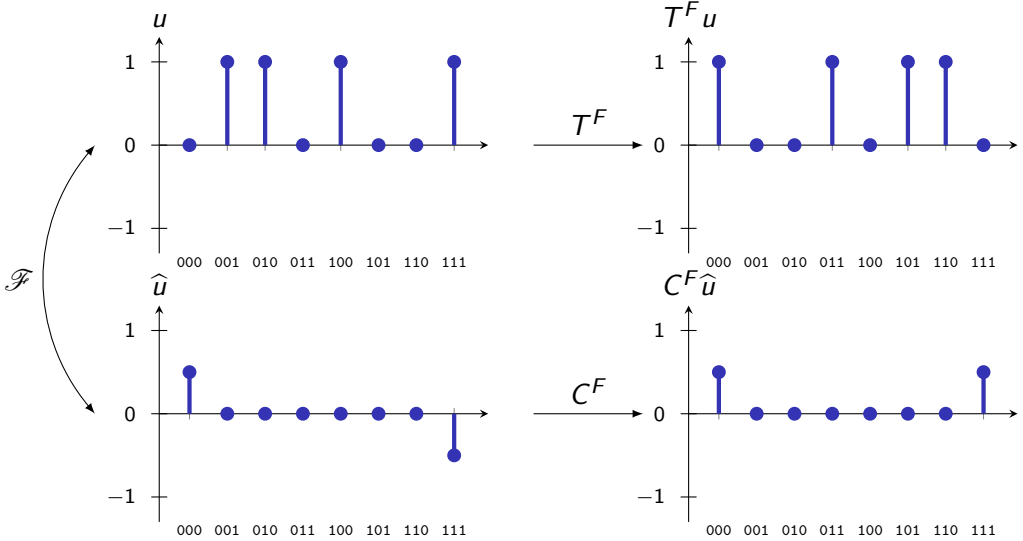
Fourier transformatie op $\mathbb{F}_2^n$

$F(x) = x + 001$



Fourier transformatie op $\mathbb{F}_2^n$

$F(x) = x + 001$



Fourier transformatie op $\mathbb{F}_2^n$

$F(x) = x + 001$

$$C^F = \begin{array}{c} \\ \\ \end{array} \begin{array}{c} \begin{array}{cccccccc} & & & & u & & & \\ 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix} \end{array} \begin{array}{l} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{array} v$$

Correlatiematrix van een functie

Substitutie $S\colon \mathbb{F}_2^3 \to \mathbb{F}_2^3$

$$C^S = \begin{array}{c} \\ \\ \end{array} \begin{array}{c} \begin{array}{cccccccc} \multicolumn{8}{c}{u} \\ 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 0 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 0 & -\frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & -\frac{1}{2} & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 & 0 & \frac{1}{2} \end{bmatrix} \end{array} \begin{array}{l} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{array} v$$

Correlatiematrix van een functie

Substitutie $S\colon \mathbb{F}_2^3 \to \mathbb{F}_2^3$

$$C^S = \begin{array}{c} \\ u \\ \end{array}$$

	000	001	010	011	100	101	110	111	
000	1	0	0	0	0	0	0	0	000
001	0	$-\frac{1}{2}$	0	$-\frac{1}{2}$	0	$\frac{1}{2}$	0	$-\frac{1}{2}$	001
010	0	0	$-\frac{1}{2}$	$\frac{1}{2}$	0	0	$-\frac{1}{2}$	$-\frac{1}{2}$	010
011	0	$\frac{1}{2}$	$-\frac{1}{2}$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	011
100	0	0	0	0	$-\frac{1}{2}$	$-\frac{1}{2}$	$\frac{1}{2}$	$-\frac{1}{2}$	100
101	0	$-\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$	0	$\frac{1}{2}$	0	101
110	0	0	$\frac{1}{2}$	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{1}{2}$	0	0	110
111	0	$-\frac{1}{2}$	$-\frac{1}{2}$	0	$-\frac{1}{2}$	0	0	$\frac{1}{2}$	111

v

Correlatiematrix van een functie

$$C^S_{011,001} = \frac{1}{8} \sum_{x \in \mathbb{F}_2^3} (-1)^{001 \cdot x + 011 \cdot S(x)} = \frac{1}{2}$$

x	000	001	010	011	100	101	110	111
$001 \cdot x$	0	1	0	1	0	1	0	1
$011 \cdot S(x)$	0	1	0	1	1	1	0	0
$(-1)^{001 \cdot x + 011 \cdot S(x)}$	$+1$	$+1$	$+1$	$+1$	-1	$+1$	$+1$	-1

Correlatiematrix van een functie

- Correlatiematrix van samengestelde functies:

$$C^{F_2 \circ F_1} = C^{F_2} C^{F_1}$$

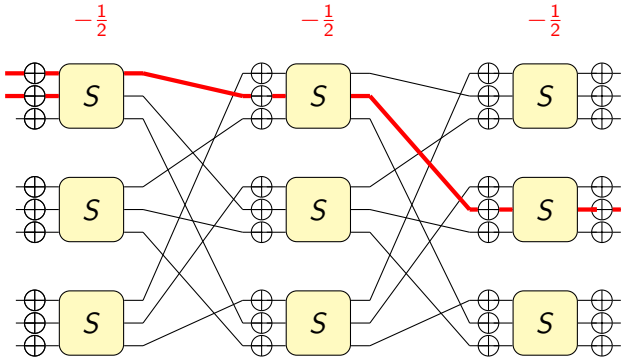
- Uitgeschreven in coördinaten voor $F = F_r \circ \cdots \circ F_2 \circ F_1$:

$$C^{F}_{u_{r+1},u_1} = \sum_{u_2,\ldots,u_r} \underbrace{\prod_{i=1}^{r} C^{F_i}_{u_{i+1},u_i}}_{\text{Correlatie van een pad}}$$

- Een tupel $(u_1, \ldots, u_{r+1})$ is een 'pad'

Paden

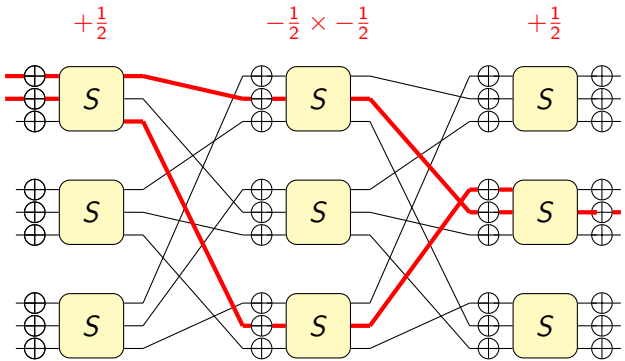
- $C^{\mathsf{E}_k}_{v,u}$ voor $(u, v) = (000000011, 000010000)$



$$C^{\mathsf{E}_k}_{v,u} = -\frac{(-1)^{\kappa_1}}{8} + \cdots$$

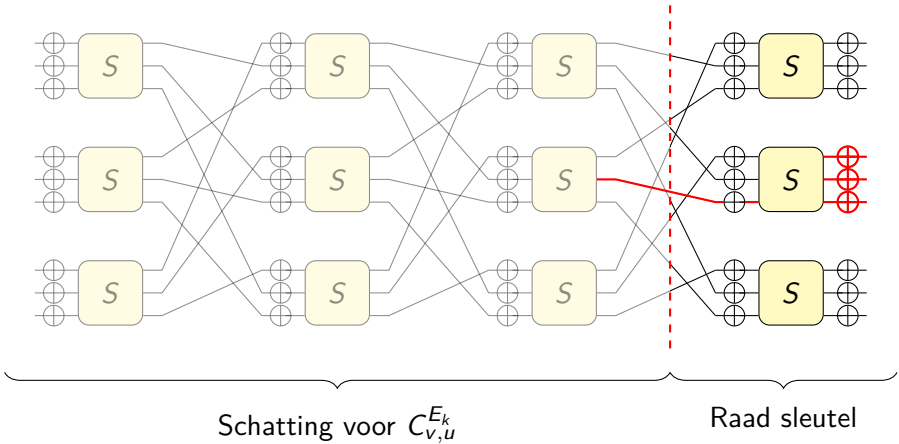
Paden

- $C_{v,u}^{\mathsf{E}_k}$ voor $(u, v) = (000000011, 000010000)$



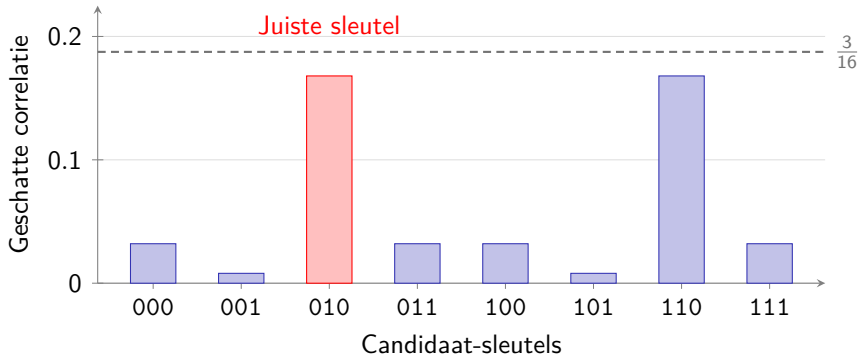
$$C_{v,u}^{\mathsf{E}_k} = -\frac{(-1)^{\kappa_1}}{8} + \frac{(-1)^{\kappa_2}}{16} = \pm \begin{cases} \frac{3}{16} & \text{als } \kappa_1 \neq \kappa_2 \\ \frac{1}{16} & \text{als } \kappa_1 = \kappa_2 \end{cases}$$

Aanval op het speelgoedcijfer



Aanval op het speelgoedcijfer

- Schat de correlatie van de benadering voor elke sleutel
- $250 > 1/c^2$ klaartekst-cijfertekst paren



Wat we hebben overgeslagen

- Andere symmetrieën bv. vermenigvuldiging (en-poort)
- Veiligheidsargumenten? Bewijzen?
- Asymmetrische cryptografie

Bedankt voor uw aandacht!

Tim Beyne

tim.beyne@esat.kuleuven.be

cryptanalysis.info

COSIC, KU Leuven
Kasteelpark Arenberg 10 bus 2452, 3001 Leuven

Appendix

TLS 1.3 (X25519, ECDSA P-256, AES-256-GCM)

```
004f ^«˜«´´´´š``` `-``␣cryptanalysis.info
0073 `␣`"^^^^^^^^^-`»`·` `·`ı`º^^^^^^^^^^`#
0097 ```-``` ```␣`$`"""*^^^^^^^^␣J`·`·```·
00bb ␣ `+^^^^^^-^^^^^3`&`$`·`
00df ␣Ï¸·øřfæzÁ.IigıðĄSĆËì¨ôu·ÁãœÛż%ůy`·`
005f ś~Y@«þ";>ź␣òhűdfË¨XöCW·l`&~>¸f·-»~~~
0083 ´´ ~~`·ùö7ïŘw¿Ī!Aežä;˜=ř¸?Ù»þ··m` ˜
```

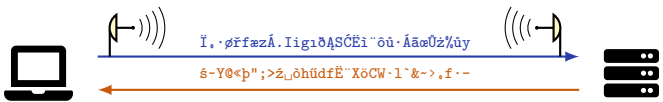
```
004f ^«˜«´´´´š``` `-``␣cryptanalysis.info
0073 `␣`"^^^^^^^^^-`»`·` `·`ı`º^^^^^^^^^^`#
0097 ```-``` ```␣`$`"""*^^^^^^^^␣J`·`·```·
00bb ␣ `+^^^^^^-^^^^^3`&`$`·`
00df ␣Ï¸·øřfæzÁ.IigıðĄSĆËì¨ôu·ÁãœÛż%ůy`·`
005f ś~Y@«þ";>ź␣òhűdfË¨XöCW·l`&~>¸f·-»~~~
0083 ´´ ~~`·ùö7ïŘw¿Ī!Aežä;˜=ř¸?Ù»þ··m` ˜
```

```
0f86 ÌŒŸ8ŮÎ©ä2XúąĄŚ®ÓW*ðđùBx^âõŮč+,W<vĹ−§
0faa àÎaŠî´Á-·\Ñ␣1Å?> ŘNJPq:ôÞŒĹÿdø¸ź1out
0fce OźĆ%ó·aĪŃ¸sìÅÊűC»ł ı*·ÜvŰ&ñzûw4ènŒOő
0ff2 i[ðŸÎ£5YdÌþO~úàèõŢTó'Č˚.¸šciýž·,ź·§·
1016 <ȷ mő´'A£íÎ·¯tÀ»HĆuČĂłyl´ekâ¸ÚúÝ˝ÎŁi
103a Ę·ĚÅ5å␣,Æ(ÁŒíú)E[žXdŒ¸<ØÕČŘ˚ČižŽÈðÉÍ
105e aŃC_ä<nÿ*ŠîlŢè»šć·VIčÔT3óBjĄvÅŽ8%¸Ík
1082 ć'ĎÑŞŃÍOŘ,RtÃ»éèŸÊw˜š¿Ů}¨LOþŃ˚a^ö"þ¡
10a6 ąÙÒV˙Ť˙YA[§\·džßD»ÉgAfĞíŮÜćê®Šâúq−*Ñ
10ca m·−'4.>ðŠÿţ˙7J=đ!øÜőšÁXź_Oëãj͡ŢĄčPùą
10ee GëŢac müĐśĘ˝˝ŻŒĎù,ĬVkÓvżaàŮÜYèÙÖo˙51
1112 Ďn)hČl¡ąÁL,8čÀŒ\ëA«ßąé#·ĽšÓ−źŽĞHŐ^ĥť
```

```
0000 HTTP/1.1␣200␣OK,˙Server:␣nginx/1.22.
0024 1,˙Date:␣Wed,␣02␣Sep␣2026␣16:14:19␣G
0048 MT,˙Content-Type:␣text/html;␣charset
006c =utf-8,˙Content-Length:␣618,˙Connect
0090 ion:␣close,˙X-Frame-Options:␣DENY,˙X
00b4 -Content-Type-Options:␣nosniff,˙Refe
00d8 rrer-Policy:␣same-origin,˙Cross-Orig
00fc in-Opener-Policy:␣same-origin,˙,```<
0120 html␣xmlns="http://www.w3.org/1999/x
0144 html"␣lang=""␣xml:lang="">`˙<head>˙<
0168 meta␣charset="utf-8"␣/>˙<meta␣name="
018c viewport"␣content="width=device-widt
```

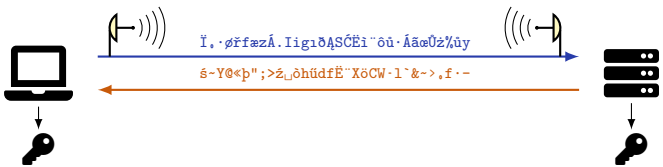
Symmetrische en asymmetrische cryptografie

- Asymmetrische cryptografie



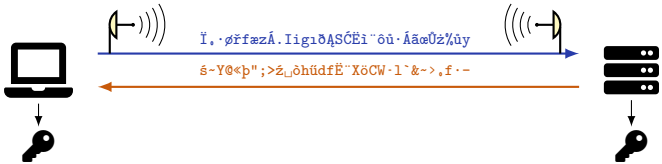
Symmetrische en asymmetrische cryptografie

- Asymmetrische cryptografie



Symmetrische en asymmetrische cryptografie

- Asymmetrische cryptografie



- Symmetrische cryptografie

