

# Stromchiffren (2)

Krypto II

VL 16

26.11.2018

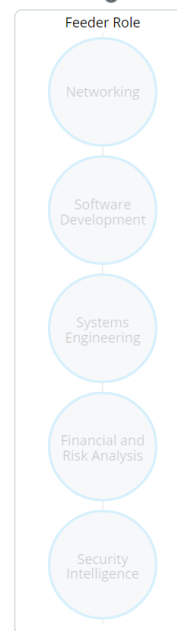
# Business Exkurs - Nützliche Infos

# Cybersecurity Career Pathway

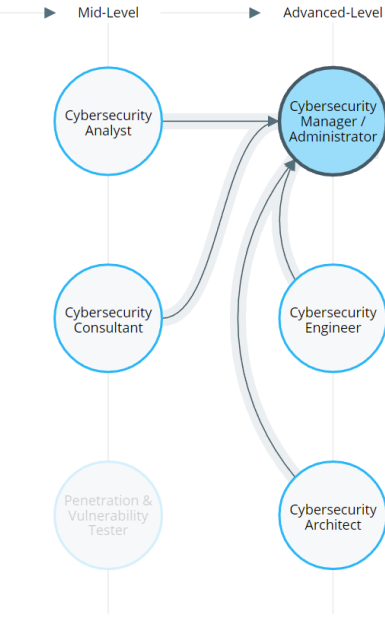
There are many opportunities for workers to start and advance their careers within cybersecurity. This interactive career pathway shows key jobs within cybersecurity, common transition opportunities between them, and detailed information about the salaries, credentials, and skillsets associated with each role.

[Share](#)
[Embed](#)

## Common Cybersecurity Feeder Roles



## Core Cybersecurity Roles



## Cybersecurity Manager / Administrator

### AVERAGE SALARY

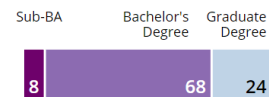
\$115,000



### COMMON JOB TITLES

- Information Security Manager
- Security Administrator
- Information Systems Security Officer
- Information Security Officer
- Information Systems Security Officer Issa

### REQUESTED EDUCATION (%)



### TOP SKILLS REQUESTED

- Information Security
- Information Systems
- Information Assurance
- Linux
- Network Security
- Project Management
- Vulnerability assessment
- NIST Cybersecurity Framework
- Security Operations

### TOTAL JOB OPENINGS

14,320



### COMMON NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORIES

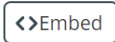
- Oversee and Govern
- Collect and Operate
- Analyze
- Securely Provision
- Operate and Maintain
- Protect and Defend

### TOP CERTIFICATIONS REQUESTED

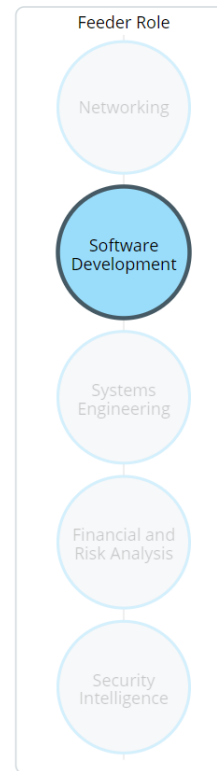
- CISSP
- CISM
- CISA
- GIAC
- Security+

# Cybersecurity Career Pathway

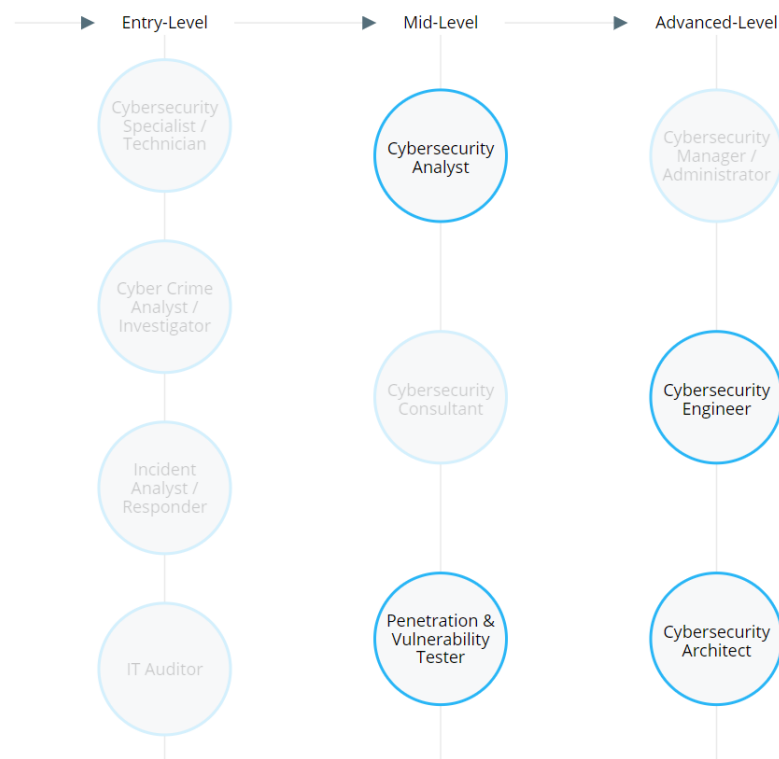
There are many opportunities for workers to start and advance their careers within cybersecurity. This interactive career pathway shows key jobs within cybersecurity, common transition opportunities between them, and detailed information about the salaries, credentials, and skillsets associated with each role.



## Common Cybersecurity Feeder Roles ⓘ



## Core Cybersecurity Roles ⓘ



## Software Development

### TOTAL JOB OPENINGS ⓘ

937,508



### COMMON JOB TITLES ⓘ

- Software Engineer
- Java Developer
- Senior Software Engineer
- .Net Developer
- Devops Engineer

### TOP SKILLS REQUESTED ⓘ

- 1 JAVA
- 2 Software Development
- 3 SQL
- 4 Software Engineering
- 5 JavaScript
- 6 Microsoft C#
- 7 LINUX
- 8 Python
- 9 Oracle

### TOP CYBERSECURITY SKILLS TO ADD ⓘ

- 1 Information Systems
- 2 Cryptography
- 3 Information Assurance
- 4 Security Operations
- 5 Routers
- 6 Risk Assessment
- 7 Switches
- 8 Risk Management
- 9 Disaster Recovery Planning

### REQUESTED EDUCATION (%) ⓘ



### TOP CERTIFICATIONS REQUESTED ⓘ

- ITIL
- Security+
- CISSP
- Project Management Certification
- GIAC

Jobs ▾

Standort

Suchen

Praktika ▾

Gepostet am ▾

Entfernung ▾

Mehr ▾

Filter zurücksetzen

Job-Mails anfordern



**Praktikum im Bereich Cyber Security - Automotive Intrusion Detection (m/w)**

WABCO – Hannover

vor 3 Tagen



**Werkstudent- Admin. Unterstützung im Bereich Cyber Security & Privacy**

Continental – Frankfurt

vor 21 Tagen



**Praktikum im Bereich Airbus Cyber Security**

Airbus – München

vor 3 Tagen



**Praktikant / Werkstudent (w/m)**

PwC – Frankfurt

vor 16 Tagen



**Assurance Internship**

Context Information Security – Deutschland


vor 2 Tagen



**Werkstudent (m/w) IT Security / Cybersecurity**

HSBC Holdings – Düsseldorf


vor 18 Tagen



**Praktikum Future Labs (m/w) IT/ Informatik/ Machine Learning**

Campusjäger GmbH – Karlsruhe

vor 6 Tagen



**Praktikant/Werkstudent (m/w) - IT Security Consulting**

Accenture – Deutschland

Schnellbewerbung

vor 2 Tagen



**Praktikant IT-Security (m/w/d)**

IABG – Ottobrunn

vor 10 Tagen



**Werkstudent Sales & Customer Approach**

Atos – Leipzig

vor 2 Tagen



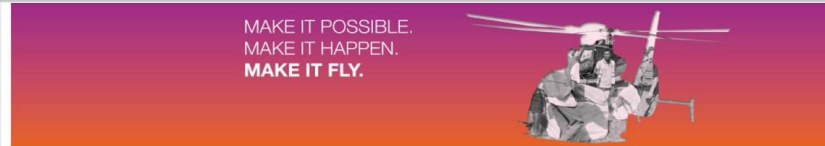
**Praktikant (m/w) Human Resources Schwerpunkt Recruiting -**

QuoScient GmbH – Frankfurt

vor 5 Tagen



**Praktikant / Werkstudent (m/w/d) Digitale Plattform**



**Praktikum im Bereich Airbus Cyber Security**

4.0 ★ Airbus – Munich, Deutschland

Jetzt bewerben

Speichern

Job Unternehmen Sterne Gehalt Bewertungen Warum wir? Zusatzleistungen

Airbus CyberSecurity Ottobrunn

Cyber Security ist für Sie mehr als nur eine Antivirus-Schutzmaßnahme? Dann sind Sie bei uns richtig! Als europäischer Spezialist auf dem Gebiet der Cyber-Sicherheit schützen wir Regierungs- und Verteidigungsorganisationen sowie kritische nationale Infrastrukturen vor aktuellen Cyber-Bedrohungen. Mit Hilfe unserer leistungsfähigen Sicherheitsprodukte und kundenorientierten Dienstleistungen können wir fortschrittlichste Cyber-Angriffe frühzeitig entdecken, analysieren und angemessen behandeln.

Description of the job

Sie sind auf der Suche nach einem Praktikum und möchten die Arbeit bei Airbus Cyber Security kennen lernen? Dann bewerben Sie sich jetzt! Wir freuen uns, wenn Sie uns in der Abteilung Service Operations als Praktikant (m/w) in Vollzeit mit 35 Stunden pro Woche (Gleitzeit) unterstützen!

Standort: Ottobrunn (München)  
Start: Frühjahr 2019  
Dauer: 6 Monate

Als Mitarbeiter von Airbus Defence and Space Cyber Security sind Sie mit Ihren Kollegen/innen als Team für die Anforderungsdefinition, Implementierung und den Betrieb von Cyber Security Lösungen sowie kundenspezifischen Dienstleistungen zuständig. Ihre Aufgaben umfassen die Mitarbeit in einem großen und interdisziplinären Team sowie die Teilnahme an operativen Internationalen Einsätzen. Internships at Airbus

Tasks & accountabilities

Wir bieten Ihnen folgende spannende Aufgaben:

- Mitarbeit im SOC / Cyber Defence Center
- Unterstützung Integrationen und Betrieb des IT-Labor
- Durchführen von Programmier- und Skript-Aufgaben
- Integrationsunterstützung von Automatisierungen
- Durchführen von Tests und Validierungen



## Robert Bosch

Arbeitgeber aktiv



Übersicht

3,3 Tsd  
Bewertungen216  
Jobs3,2 Tsd  
Gehälter848  
Vorstellungsgespräche812  
Zusatzleistungen44  
Fotos

Beobachten

+ Gehalt posten

## Gehälter bei Robert Bosch

1439 Gehälter (für 634 Stellenbezeichnungen) Aktualisiert am 24. Nov 2018

Wie viel verdienen Mitarbeiter bei Robert Bosch? Glassdoor bietet Angaben zu Löhnen, Gehältern und Boni, die auf Beiträgen von Mitarbeitern und Schätzwerten beruhen.

Jobtitel

Deutschland

Suchen

Sortieren: Meiste Gehaltsberichte | Gehalt

Durchschn. Grundgehälter (in EUR)

Niedrig

Hoch

## Praktikant - Pro Monat

132 Gehälter

971 €/Mon.

565 €

2 Tsd €

## Masterand - Pro Monat

45 Gehälter

730 €/Mon.

700 €

800 €

## Entwicklungsingenieur

39 Gehälter

74.759 €/Jahr

46 Tsd €

95 Tsd €



Sind diese Infos hilfreich? Die Community freut sich über jeden Beitrag – Gehalt anonym angeben

## Praktikum - Pro Monat

38 Gehälter

975 €/Mon.

676 €

1 Tsd €



Cyber Security Professional  
(m/w/d)  
Siemens PLC – München



Cyber Security Specialist (w/m)  
Airbus – München

Empfohlene Jobs

## Werkstudent - Pro Stunde

34 Gehälter

16 €/Std.

12 €

17 €

## Werkstudent - Pro Monat

31 Gehälter

679 €/Mon.

525 €

740 €

## Intern - Pro Monat

22 Gehälter

964 €/Mon.

750 €

1 Tsd €



Sie arbeiten im Bereich HR  
oder Marketing?

Kostenloses Arbeitgeberkonto  
freischalten

## Jobs, die Sie interessieren könnten



Berater (w/m/d) Governance  
Cyber Security  
Deutsche Bahn – Berlin



Cyber Security Architect  
Software House  
Luxoft – Berlin



Cyber Security Engineer  
(m/w)  
Airbus – München



(Senior) Manager (w/m)  
Informationssicherheit /  
Cyber Security...  
MHP - A Porsche Company –  
München



Werkstudent (m/w/divers)  
Cyber Security  
Siemens PLC – München



Consultant Cyber Security  
(w/m)  
Sulzer GmbH – München



Consultant (w/m) Cyber  
Security  
PwC – München















Cyber Security Manager  
Verizon – Dortmund



Head of Cyber Security (m/f)  
QIAGEN – Hilden



Spezialist Cyber Security

-  Bundesnachrichtendienst BND – Berlin vor 3 Tagen
-  **Informatiker / Ingenieur für Cyber-Sicherheit (m/w) - IT-Security, IT** Bundesnachrichtendienst BND – Berlin vor 3 Tagen
-  **Satelliten- und Luftbildauswerter (m/w) (Bachelor/FH)** Bundesnachrichtendienst – Pullach i. Isartal vor 15 Tagen
-  **Medientechnologie Druck (m/w)** Bundesnachrichtendienst – Pullach i. Isartal vor 19 Tagen
-  **Informatiker und Ingenieure (m/w) (FH/Bachelor)** Bundesnachrichtendienst (BND) – München vor 20 Tagen
-  **Elektroniker (m/w)** Bundesnachrichtendienst – Pullach i. Isartal vor 15 Tagen
-  **Informatiker, Ingenieure und Mathematiker (m/w) (FH/Bachelor)** Bundesnachrichtendienst (BND) – Berlin vor 20 Tagen
-  **Informatiker und Ingenieure (m/w) - Entwicklung, Ingenieur** Bundesnachrichtendienst BND – Garching b.München vor 30+ Tagen
-  **Experte für Cyber-Sicherheit (m/w) (Bachelor/FH)** Bundesnachrichtendienst – Pullach i. Isartal vor 19 Tagen
-  **Informatiker / Ingenieur für Cyber-Sicherheit (m/w) (Master/Diplom)** Bundesnachrichtendienst – Pullach i. Isartal vor 19 Tagen
-  **Bauingenieur (m/w) (Bachelor/FH)** Bundesnachrichtendienst – Pullach i. Isartal vor 19 Tagen
-  **Verwaltungsfachwirt für Haushalt und Vergabe (m/w) (Bachelor/FH)** Bundesnachrichtendienst – Pullach i. Isartal vor 19 Tagen

**Experte für Cyber-Sicherheit (m/w) (Bachelor/FH)** Bundesnachrichtendienst

Jetzt bewerbenSpeichern

JobUnternehmen

- Internationale Kooperationen

**Anforderungsprofil**

- abgeschlossenes wissenschaftliches Hochschulstudium (Bachelor/FH) in einem der folgenden Studiengänge
  - Informatik
  - Elektro-/Informations-/Nachrichtentechnik
  - Wirtschaftsingenieurwesen
  - Maschinenbau
  - Naturwissenschaften (Physik, Chemie, Biologie)
- grundlegendes Verständnis der Informationstechnik und der Cyber-Sicherheit
- gute Englischkenntnisse in Wort und Schrift
- ausgeprägte analytische Fähigkeiten
- gute schriftliche und mündliche Ausdrucksfähigkeit
- Team- und Kommunikationsfähigkeit
- Eigeninitiative, Gewissenhaftigkeit und Zuverlässigkeit
- Bereitschaft zur Fort- und Weiterbildung
- Bereitschaft zu Dienstreisen im In- und Ausland
- deutsche Staatsangehörigkeit

**Besondere Hinweise**

Im Interesse der beruflichen Gleichstellung sind Bewerbungen von Frauen in Bereichen mit Unterrepräsentanz besonders erwünscht und werden bei gleicher Eignung, Befähigung und fachlicher Leistung nach Maßgabe des BGleGlG bevorzugt berücksichtigt.

Schwerbehinderte Menschen werden bei gleicher Eignung, Befähigung und fachlicher Leistung nach Maßgabe des SGB IX und der für den Geschäftsbereich des BND geschlossenen Integrationsvereinbarung bevorzugt berücksichtigt.

Bitte behandeln Sie Ihre Bewerbung diskret und beachten hierzu die Hinweise auf unserer Homepage unter [www.karriere.bund.de](http://www.karriere.bund.de).

**Arbeitgeber-Leistungen**

- Vergütung erfolgt je nach Qualifikation im vergleichbar gehobenen Dienst gemäß Tarifvertrag für den öffentlichen Dienst (TVöD Bund) in den Entgeltgruppen E10 - E13
- Zahlung einer tariflichen Sonderzulage in einer Höhe von bis zu 1000 € monatlich möglich

# Buch des Tages

**Titel:** Cryptography

**Autor(en):** William J. Buchanan

**Verlag:** River Publishers, 2017

**Umfang:** ca. 390 Seiten

## **Hinweise zum Inhalt:**

Das Lehrbuch ist aus einer Vorlesung entstanden, teilweise wurden bunte Folien und Bildschirm-Screenshots in den Text integriert. Die Qualität der Darstellung variiert, nützlich sind die praxisnahen Beispiele. Ferner behandelt der Autor in seinem Buch auch Themen, die üblicherweise nicht Teil einer Einführung in die Kryptographie sind, so beispielsweise Wireless Cryptography, Blockchain und Cryptocurrency, oder Tunneling. Als Kauf eher nicht empfohlen, zur Ausleihe – falls verfügbar – aber durchaus eine gute Ergänzung anderer Lehrbücher.



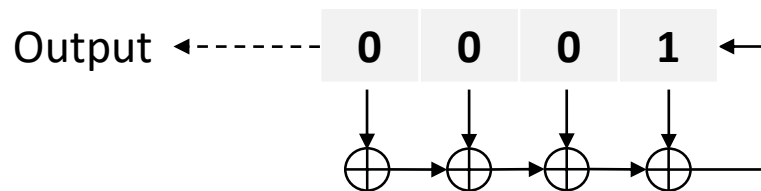
# Beispiel für LFSR (1)

Wir betrachten einfache Beispiele für ein lineares Feedback Shift Register mit einer Registerlänge von 4 Bit.

## Beispiel:

Im nachfolgenden Beispiel ist  $S_0 = (0, 0, 0, 1)$  und

$f(S_i) = \sum_{j=1}^4 a_j \cdot b_j$ , wobei  $a_j = 1$  für alle  $j = 1, \dots, 4$ .



Wir erhalten  $f(S_0) = f(0, 0, 0, 1) = 0 \oplus 0 \oplus 0 \oplus 1 = 1$

$\Rightarrow S_1 = (0, 0, 1, 1)$

# Beispiel für LFSR (2)

$$f(S_1) = f(0, 0, 1, 1) = 0 \oplus 0 \oplus 1 \oplus 1 = 0$$

$$\Rightarrow S_2 = (0, 1, 1, 0)$$

$$f(S_2) = f(0, 1, 1, 0) = 0 \oplus 1 \oplus 1 \oplus 0 = 0$$

$$\Rightarrow S_3 = (1, 1, 0, 0)$$

$$f(S_3) = f(1, 1, 0, 0) = 1 \oplus 1 \oplus 0 \oplus 0 = 0$$

$$\Rightarrow S_4 = (1, 0, 0, 0)$$

$$f(S_4) = f(1, 0, 0, 0) = 1 \oplus 0 \oplus 0 \oplus 0 = 1$$

$$\Rightarrow S_5 = (0, 0, 0, 1) = S_0.$$

Wir haben also eine Periode der Länge 5. Maximal mögliche Periode bei einem Register der Länge 4 wäre  $n = 2^4 - 1 = 15$  gewesen.

# Beispiel für LFSR (3)

Was geschieht, wenn wir einen Startwert für unser LFSR wählen, der nicht im vorherigen Zyklus enthalten war?

Wir hatten bereits

$(0, 0, 0, 1), (0, 0, 1, 1), (0, 1, 1, 0), (1, 1, 0, 0), (1, 0, 0, 0), (0, 0, 0, 1)$

Wählen wir stattdessen  $S_0 = (0, 0, 1, 0)$ , so erhalten wir den Zyklus  
 $(0, 0, 1, 0), (0, 1, 0, 1), (1, 0, 1, 0), (0, 1, 0, 0), (1, 0, 0, 1), (0, 0, 1, 0)$

Als nächstes versuchen wir  $S_0 = (1, 1, 1, 1)$  und erhalten den Zyklus  
 $(1, 1, 1, 1), (1, 1, 1, 0), (1, 1, 0, 1), (1, 0, 1, 1), (0, 1, 1, 1), (1, 1, 1, 1)$

Unser LFSR erzeugt also drei Zyklen der Länge 5.

# Weiteres LFSR mit längerer Periode (1)

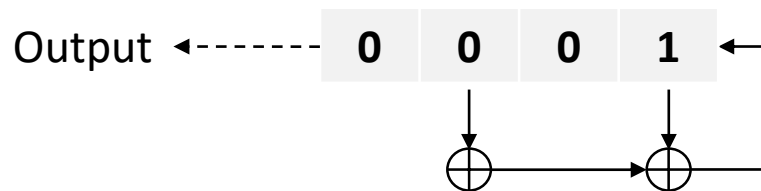
Wir betrachten ein weiteres LFSR mit einer Registerlänge von 4 Bit. Diesmal gehen Positionen  $b_1$  und  $b_3$  in die Berechnung ein:

$$f(S_i) = b_1 \oplus b_3$$

Beginnen wir diesmal mit  $S_0 = (1, 0, 0, 1)$ .

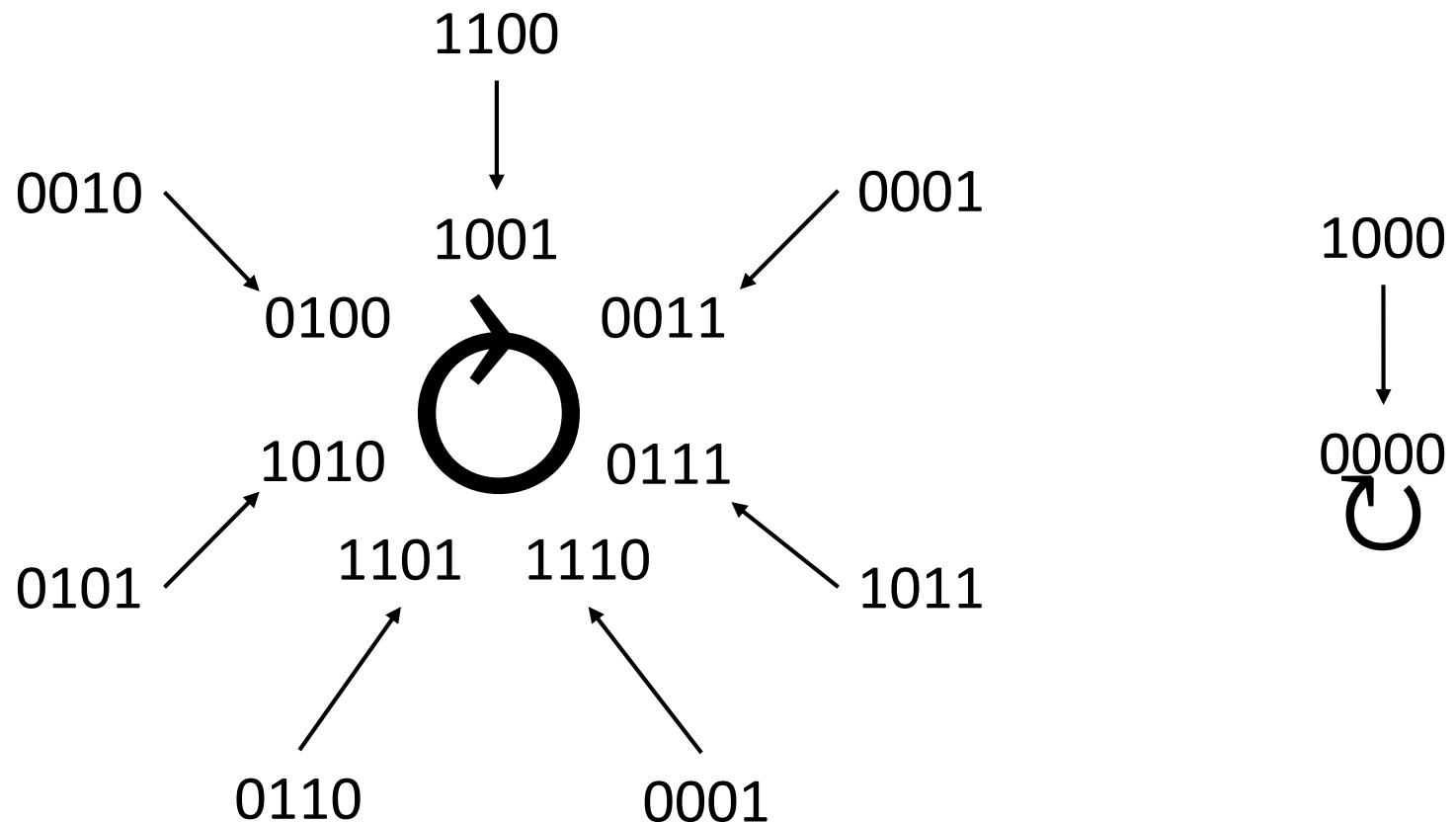
Wir erhalten  $f(S_0) = 0 \oplus 1 = 1$

$\Rightarrow S_1 = (0, 0, 1, 1)$



Wir berechnen nun die weiteren Registerzustände [siehe Tafel]

# Weiteres LFSR mit längerer Periode (2)

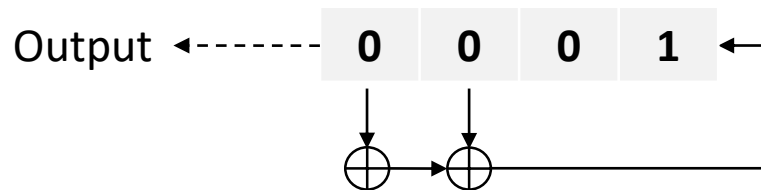


# LFSR mit maximaler Periode (1)

Wir betrachten ein zweites LFSR und untersuchen dessen Periodenlänge.

Wieder sei  $S_0 = (0, 0, 0, 1)$ , doch wir definieren nun

$$f(S_i) = \sum_{j=1}^4 a_j \cdot b_j, \text{ wobei } a_1 = a_2 = 0, a_3 = a_4 = 1.$$



Wir erhalten  $f(S_0) = f(0, 0, 0, 1) = 0 \oplus 0 = 0$

# LFSR mit maximaler Periode (2)

$$\Rightarrow S_1 = (0, 0, 1, 0)$$

Die nächsten Schritte ergeben

$$S_2 = (0, 1, 0, 0)$$

$$S_3 = (1, 0, 0, 1)$$

und als weitere:

$(0, 0, 1, 1), (0, 1, 1, 0), (1, 1, 0, 1), (1, 0, 1, 0), (0, 1, 0, 1), (1, 0, 1, 1),$   
 $(0, 1, 1, 1), (1, 1, 1, 1), (1, 1, 1, 0), (1, 1, 0, 0), (1, 0, 0, 0), (0, 0, 0, 1)$

Das letzte Element ist identisch mit  $S_1$ , so dass sich unser Zyklus nach insgesamt 15 Elementen wiederholt.

Wir haben also ein LFSR gefunden mit maximal möglicher Periodenlänge.

# Zustandsvariablen als Terme

Betrachten wir nochmals das vorhergehende LFSR, diesmal jedoch ohne die Gleichungen direkt anhand der konkreten Registerinhalte auszurechnen. Wieder sei  $f(S_i) = b_3 \oplus b_4$ . Die Terme werden zwar länger, lassen sich jedoch kürzen und haben immer maximal 4 Variablen:

$b_4$	$b_3$	$b_2$	$b_1$
-------	-------	-------	-------

$b_3$	$b_2$	$b_1$	$b_3 \oplus b_4$
-------	-------	-------	------------------

$b_2$	$b_1$	$b_3 \oplus b_4$	$b_2 \oplus b_3$
-------	-------	------------------	------------------

$b_1$	$b_3 \oplus b_4$	$b_2 \oplus b_3$	$b_1 \oplus b_2$
-------	------------------	------------------	------------------

$b_3 \oplus b_4$	$b_2 \oplus b_3$	$b_1 \oplus b_2$	$b_1 \oplus b_3 \oplus b_4$
------------------	------------------	------------------	-----------------------------

$b_2 \oplus b_3$	$b_1 \oplus b_2$	$b_1 \oplus b_3 \oplus b_4$	$b_2 \oplus b_3 \oplus b_3 \oplus b_4$
------------------	------------------	-----------------------------	--

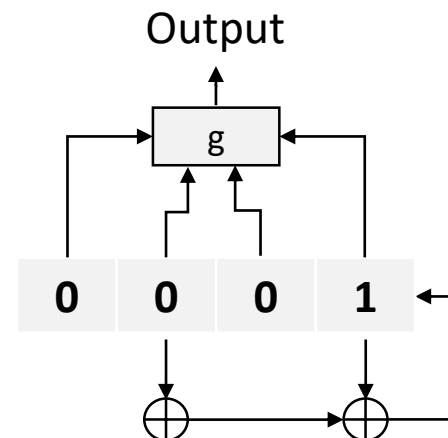
$b_1 \oplus b_2$	$b_1 \oplus b_3 \oplus b_4$	$b_2 \oplus b_3 \oplus b_3 \oplus b_4$	$b_1 \oplus b_2 \oplus b_2 \oplus b_3$
------------------	-----------------------------	--	--



# Gefilterte Linear Feedback Shift Register

- Wie wir bereits wissen, sind LFSR in ihrer Verwendung als Stromchiffre für kryptographische Zwecke nicht geeignet. Sie bilden jedoch nützliche Komponenten für die Konstruktion sicherer Stromchiffren.
- Ein Lösungsansatz, der sich jedoch nicht bewährt hat, sind sogenannte ***Gefilterte Lineare Feedback Shift Register***.

Beispiel:



- Dabei wird die Nichtlinearität hinzugefügt in Form einer nichtlinearen Funktion  $g$ . Der Output erfolgt durch die Funktion  $g$ , nicht durch den Registerinhalt.

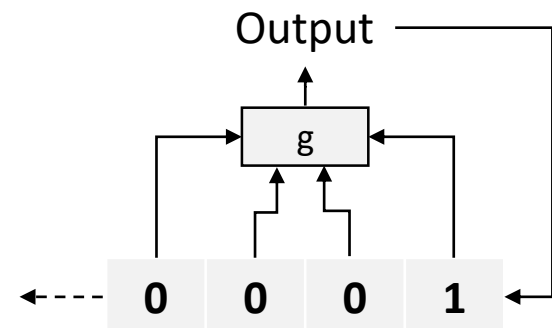
# Angriffe auf Gefilterte LFSR

Es würde den Rahmen der VL sprengen, Details zu Angriffsmethoden auf Gefilterte LFSR darzustellen, insbesondere müsste wir zuvor weitere mathematische Hilfsmittel einführen. Dennoch, ohne Details, nur zur Info, in aller Kürze:

- ***Fast Correlation Attacks***: versuchen die Anwendung von Lösungsverfahren für lineare Gleichungen auf die nichtlineare Filterfunktion  $g$ .
- ***Cube Attacks***: betrachten Ableitungen nichtlinearer Gleichungen mit dem Ziel, den Grad der entstehenden Polynome zu reduzieren bis auf Grad eins, um lineare Systeme zu erhalten.
- ***Algebraic Attacks***: beschreiben die Output Bits als (nichtlineare) Funktionen der Registerinhalte und versuchen eine Lösung der so erhaltenen Gleichungen.

# Nichtlineare Feedback Shift Register

- Nichtlineare Feedback Shift Register sind vergleichbar aufgebaut wie die lineare Variante, nur dass die Bits im Register nicht (nur) per XOR miteinander verknüpft werden, sondern auch mithilfe nichtlinearer Operationen wie beispielsweise AND und OR.
- Die Nichtlinearität sorgt dafür, dass im Gegensatz zu LFSR (siehe Folie “Zustandsvariablen als Terme”) beliebig komplexe Terme hoher Ordnung entstehen, die nicht einfach lösbar sind.
- Es kann allerdings sehr schwierig oder gar unmöglich sein, die Periodenlänge eines nichtlinearen Feedback Shift Registers zu bestimmen.



# eStream Competition

- Öffentliche Wettbewerbe zur Identifizierung von Kryptoalgorithmen für den praktischen Einsatz gab es nicht nur in den USA, wo beispielsweise AES als Gewinner unter den eingereichten Blockchiffren hervorging.
- In Europa gab es von 2000 bis 2003 das NESSIE Projekt (New European Schemes for Signatures, Integrity and Encryption). Ziel war die Identifizierung von Cryptographic Primitives. Teilnehmer waren zahlreiche anerkannte Kryptographen. Hier wurden auch sechs Stromchiffren eingereicht und analysiert. ALLE Kandidaten wurden jedoch geknackt und schieden aus.
- Ein zweiter europäischer Anlauf in Rahmen eines erneuten Wettbewerbs, diesmal ausschließlich für Stromchiffren, folgte von 2004 bis 2008 unter dem Namen ***eStream Competition***.

## The eSTREAM Project

GENERAL INFORMATION
Home
eSTREAM Portfolio
End of Phase 3
Timetable
Technical background
Announcements

INTERACTION
Discussion Forum
Submitting Papers

DOCUMENTS
List of all papers
Software performance
Hardware performance
Statistical testing

eSTREAM workshops
SASC 2004
SKEW 2005
SASC 2006
SASC 2007
SASC 2008

ALL THE CANDIDATES
Profile 1 (SW)
Profile 2 (HW)

ABOUT THIS SITE
Who to contact
Disclaimer

This is the home page for eSTREAM, the ECRYPT Stream Cipher Project. This multi-year effort running from 2004 to 2008 has identified a portfolio of promising new stream ciphers. All information on the stream cipher project can be found on this site, including a [timetable](#) of the project and further [technical background](#) on the project.

We would like to thank everyone that contributed to eSTREAM in any way. For the future, we expect that research on the eSTREAM submissions in general, and the portfolio ciphers in particular, will continue. We therefore welcome any ongoing contributions to any of the eSTREAM submissions. It is also possible that changes to the eSTREAM portfolio might be needed in the future. If so, any future revisions will be made available via these pages.

A list of all announcements can be found [here](#). The most recent ones are listed below:

- **The current eSTREAM Portfolio**

The eSTREAM portfolio contains the following ciphers:

Profile 1 (SW)	Profile 2 (HW)
HC-128	Grain v1
Rabbit	MICKEY v2
Salsa20/12	Trivium
SOSEMANUK	

The 2009 annual review of the eSTREAM portfolio is available [here](#). The eSTREAM portfolio was revised on September 8, 2008. Details of this first revision can be found [here](#).

A short report on the portfolio and the end of eSTREAM can be found [here](#).

- **Phase 3 candidates:**

Profile 1 (SW)	Profile 2 (HW)
CryptMT (CryptMT Version 3)	DECIM (DECIM v2 and DECIM-128)
Dragon	Edon80
HC (HC-128 and HC-256)	F-FCSR (F-FCSR-H v2 and F-FCSR-16)
LEX (LEX-128, LEX-192 and LEX-256)	Grain (Grain v1 and Grain-128)
NLS (NLSv2, encryption-only)	MICKEY (MICKEY 2.0 and MICKEY-128 2.0)
Rabbit	Moustique
Salsa20	Pomaranch (Pomaranch Version 3)
SOSEMANUK	Trivium