PSL UNIVERSITÉ PARIS

THÈSE DE DOCTORAT
DE L'UNIVERSITÉ PSL

Préparée à l'École Normale Supérieure de Paris

ENS | PSL ingenico

Sécurité des applications sur systèmes non maîtrisés.

Étude des risques, protections, enjeux et intérêts autour de la confiance dans les produits informatiques sur étagère.

Soutenue par
Vincent Giraud
Le 26 septembre 2024

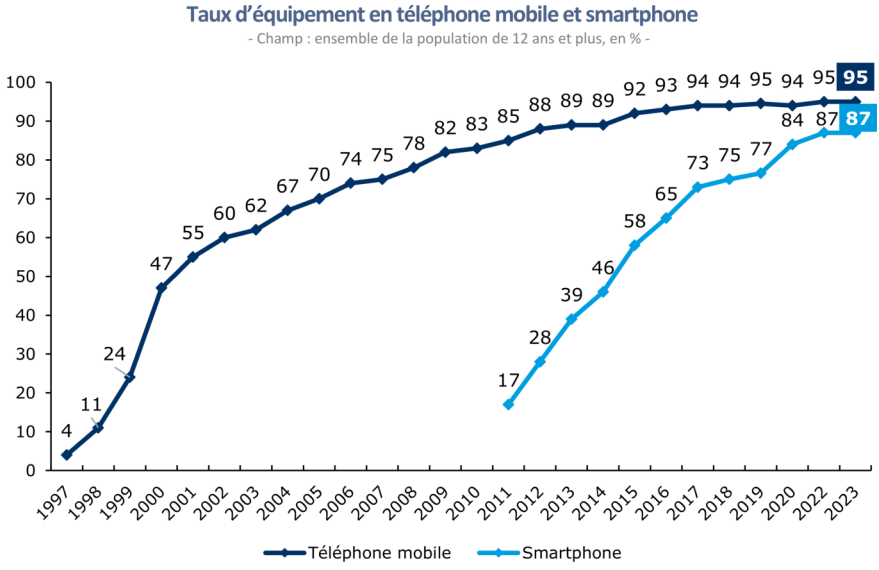
École doctorale n°386
Sciences Mathématiques de Paris Centre

Spécialité
Informatique

Composition du jury :

Pascal Lafourcade Professeur, Université Clermont Auvergne	*Rapporteur*
Clémentine Maurice Chargée de recherche HDR, CNRS, Lille	*Rapporteuse*
Aurélien Francillon Professeur, EURECOM Sophia Antipolis	*Examinateur*
Sophie Quinton Chargée de recherche, Inria Grenoble	*Examinatrice*
Guillaume Bouffard Ingénieur de recherche, ANSSI, Paris	*Co-encadrant*
David Naccache Professeur, École Normale Supérieure de Paris	*Directeur de thèse*
Tania Richmond Maîtresse de conférences, Université de la Nouvelle-Calédonie	*Invitée*

Contexte



CRÉDOC, *Baromètre du numérique*, 2023.

*La définition admise par tous est qu'un COTS (*Commercial Off The Shelf*) est un composant issu du marché ou plus communément appelé un composant sur étagère.*

Philippe Roose. *SI-COTS : Aide à l'intégration de COTS Products*, 2009.

A general-purpose mobile computing device (e.g., smartphone or tablet) that is not designed solely for the purposes of payment acceptance.

PCI Security Standards Council. *Mobile Payments on COTS*, 2023.

- Communications sécurisées

- Communications sécurisées
- Stockage sécurisé

- Communications sécurisées
- Stockage sécurisé
- Biométrie

- Communications sécurisées
- Stockage sécurisé
- Biométrie
- Authentification

- Communications sécurisées
- Stockage sécurisé
- Biométrie
- Authentification

WebAuthn

- Communications sécurisées
- Stockage sécurisé
- Biométrie
- Authentification
- Transport

- Communications sécurisées
- Stockage sécurisé
- Biométrie
- Authentification
- Transport
- Paiement

Embedded microprocessor applications all share one common trait : the end product is not a computer. The user may not realize that a computer is included (...). The teenager watching MTV is unaware that embedded computers control the cable box and the television. (...)
For the purpose of this book, an embedded system is any application where a dedicated computer is built right into the system.

Jack G. Ganssle. *The Art of Programming Embedded Systems*, 1991.

Embedded systems are computing systems dedicated to specific tasks. In many cases, the work being done was originally done by custom logic.

Alfredo Romagosa. *Embedded Systems Journal : Cache Coherence Issues for Real-Time Multiprocessing*, 1997.

Un système embarqué est un système informatique logiciel et matériel enfoui dans un objet afin de contrôler son activité et sa sécurité, d'offrir des services à ses utilisateurs et de communiquer avec d'autres objets.

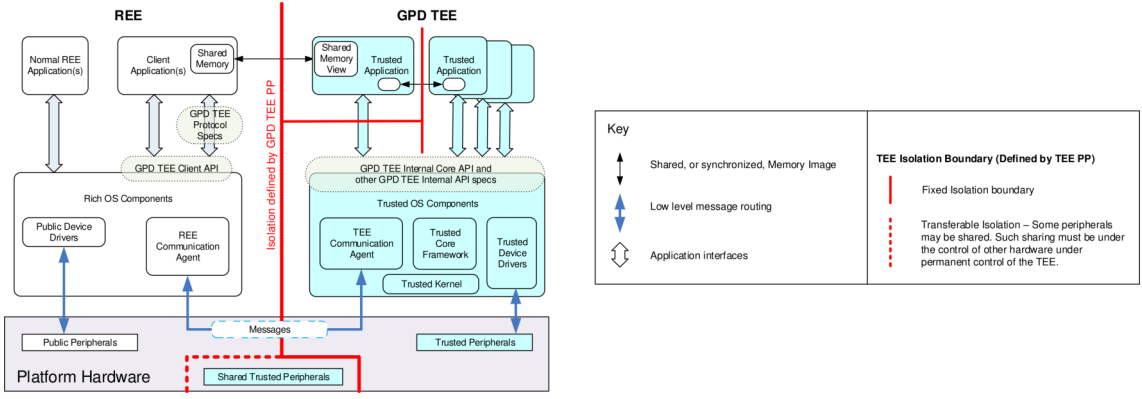
Gérard Berry. *Pourquoi et comment le monde devient numérique*, 2008.

Un objet communicant permet à l'utilisateur d'accéder à des services via cet objet grâce à un échange d'informations avec le monde qui l'entoure.
Les dispositifs numériques qui permettent d'offrir ces services sont appelés systèmes embarqués.

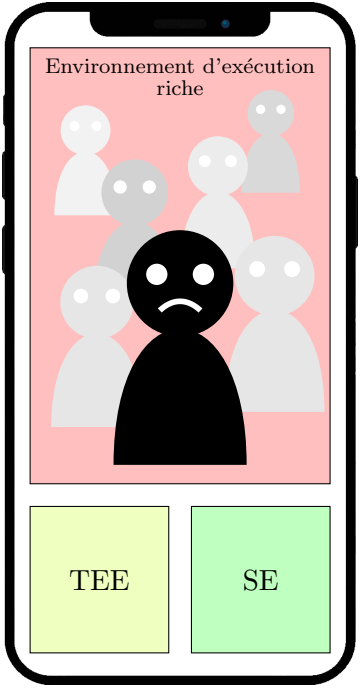
Didier Hallépée. *La sécurité du smartphone et des systèmes embarqués*, 2012.

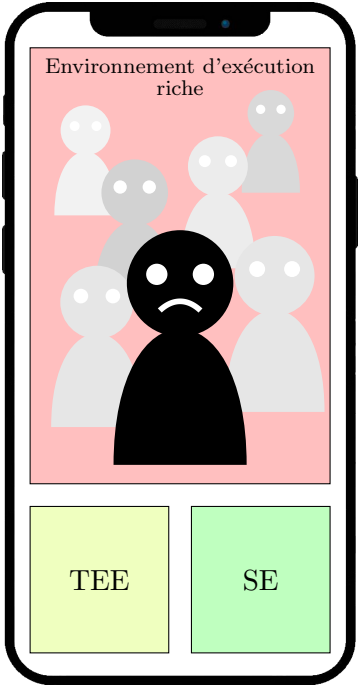
Secure Elements (SE)

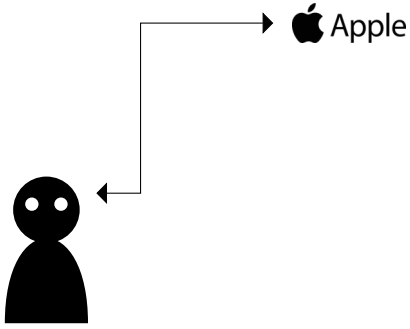
Trusted Execution Environments (TEE)

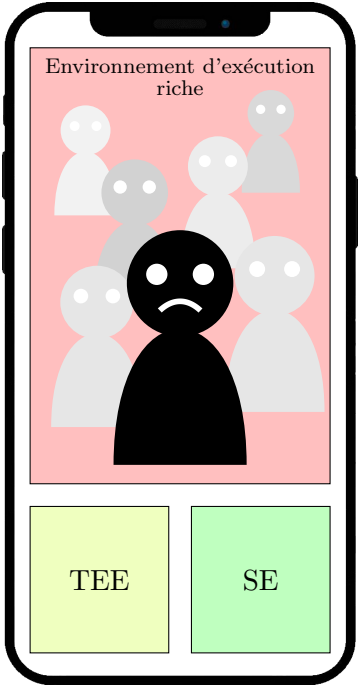


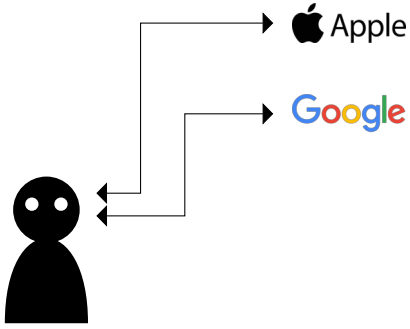
GlobalPlatform, Inc. *TEE Protection Profile*, 2020.

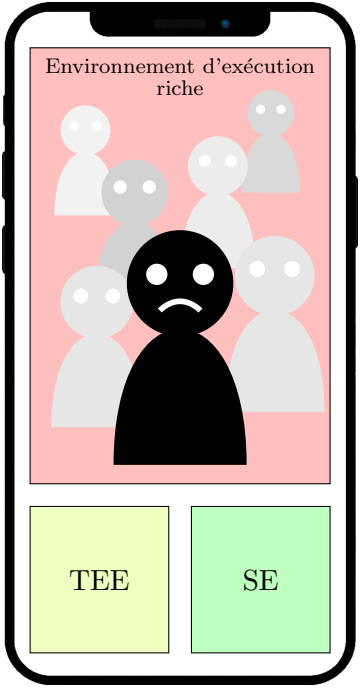

Environnement d'exécution riche
TEE
SE

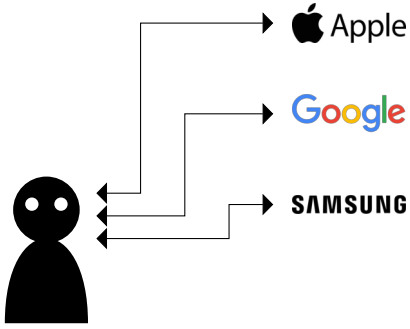

Environnement d'exécution riche
TEE
SE

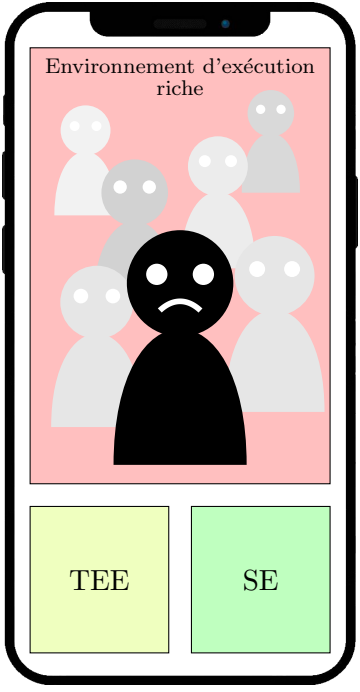

Apple

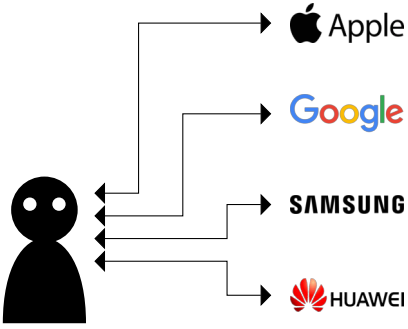

Environnement d'exécution riche
TEE
SE

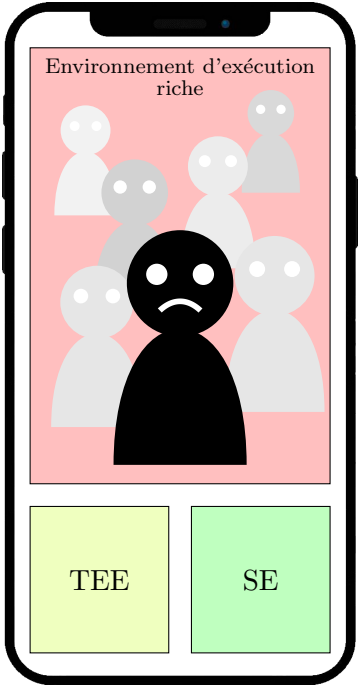

Apple
Google

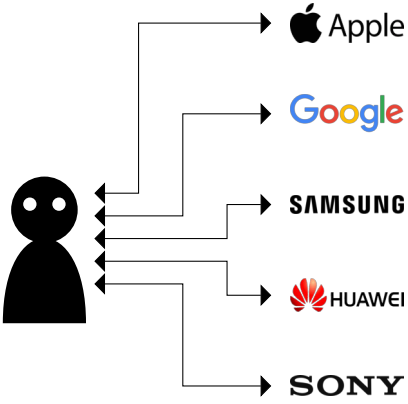

Environnement d'exécution riche
TEE
SE

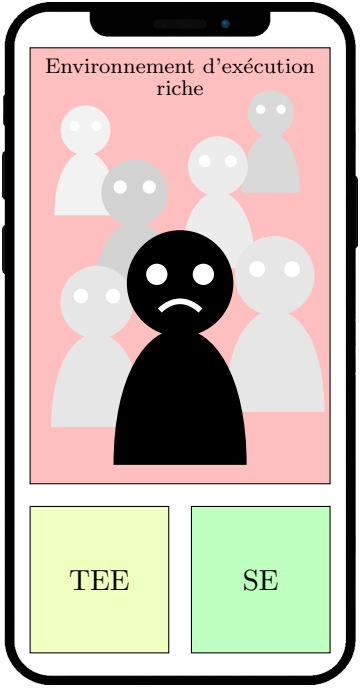

Apple
Google
SAMSUNG

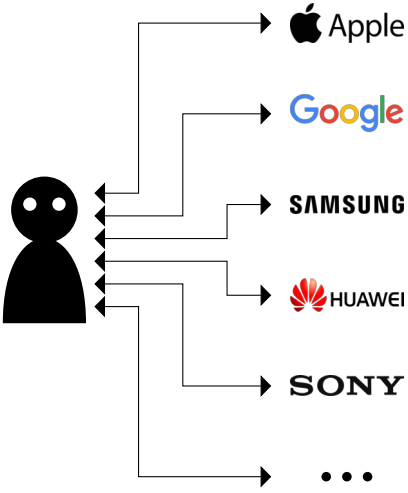

Environnement d'exécution riche
TEE
SE


Apple
Google
SAMSUNG
HUAWEI


Environnement d'exécution riche
TEE
SE


Apple
Google
SAMSUNG
HUAWEI
SONY

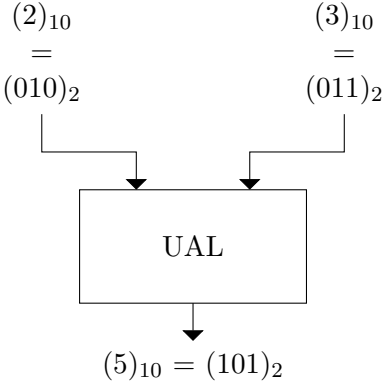

Environnement d'exécution riche
TEE
SE


Apple
Google
SAMSUNG
HUAWEI
SONY

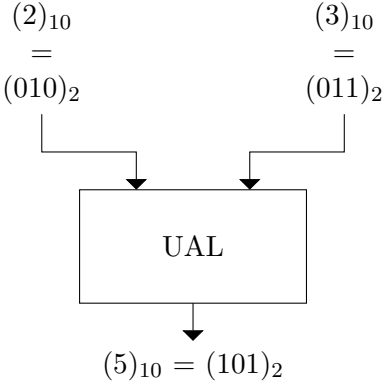
État de l'art

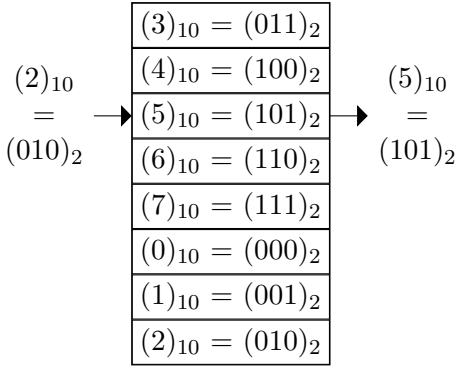
Cryptographie en boîte blanche

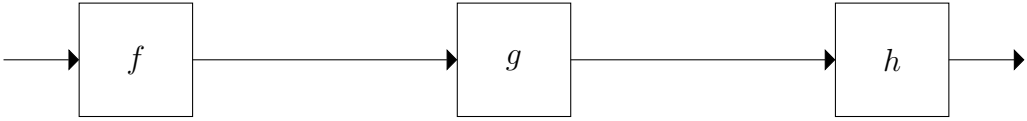
[Cho+03b ; Cho+03a]

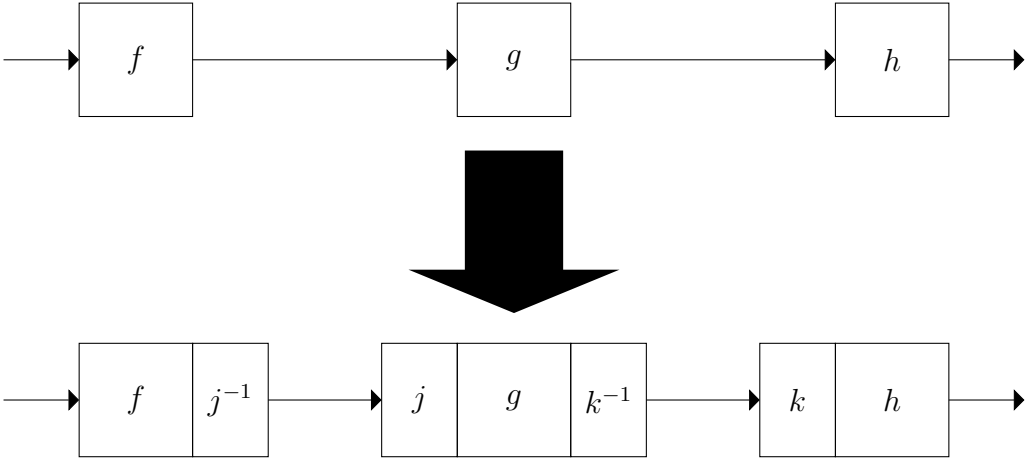


[Cho+03b ; Cho+03a]





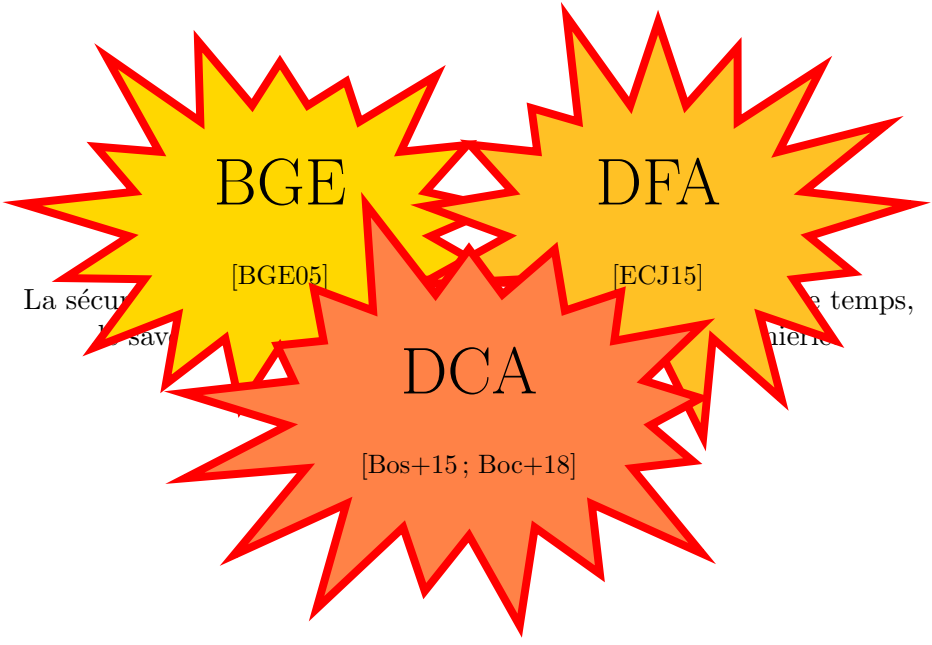

f
g
h


f
g
h
f
j^{-1}
j
g
k^{-1}
k
h

La sécurité des implémentations en boîte blanche repose sur le temps, le savoir-faire et le coût que nécessite leur rétro-ingénierie.

La sécu en boîte blanche repose sur le temps,
le sav qu écessite leur rétro-ingénierie.

La sécu en bo e temps,
sav qu écessit ière



La sécu e temps,
sav ière

PCI Security Standards Council

2.5 PIN Encryption	
Requirements	**Guidance**
6. Where white-box cryptography is used, the white-box cryptography keys must be changed monthly, at a minimum.	*Frequently changing the white-box encryption keys used to protect data substantially increases the security of the solution. When encryption is performed in software, it is critical to change the white-box key often to prevent unauthorized disclosure.*

État de l'art

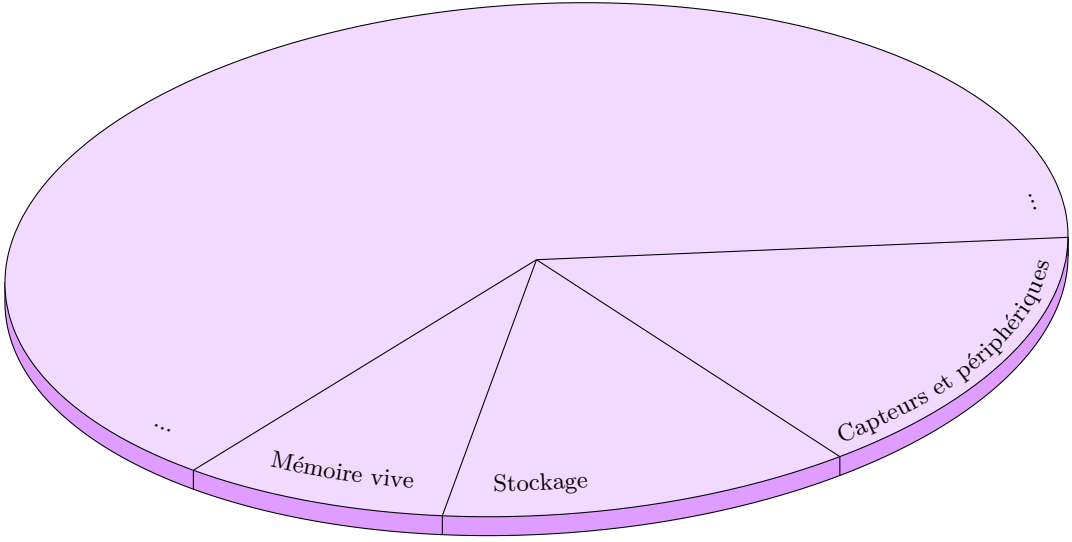
Sécurité dans Android

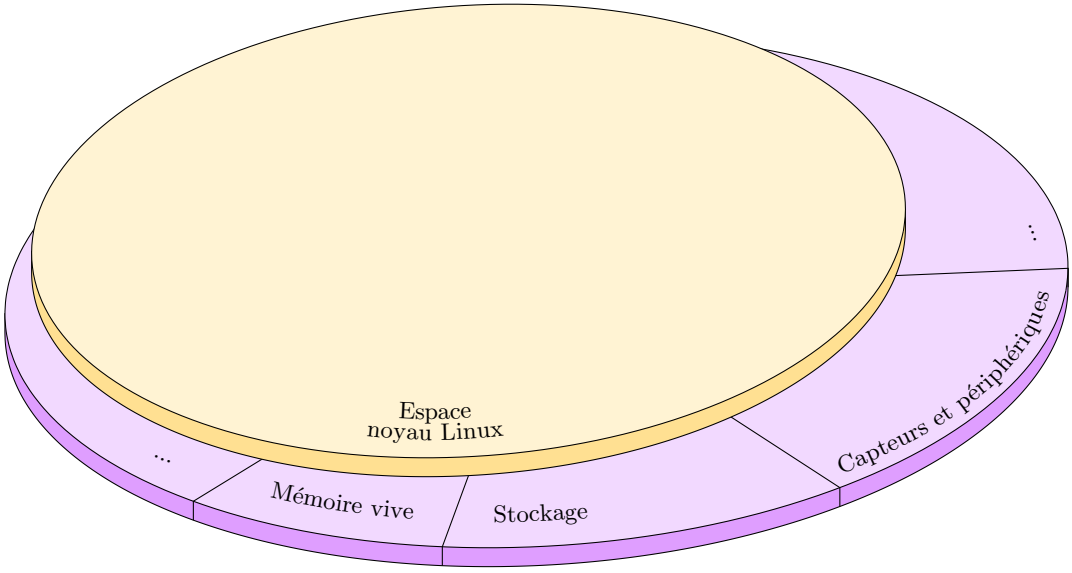
- Applications dangereuses pour le système

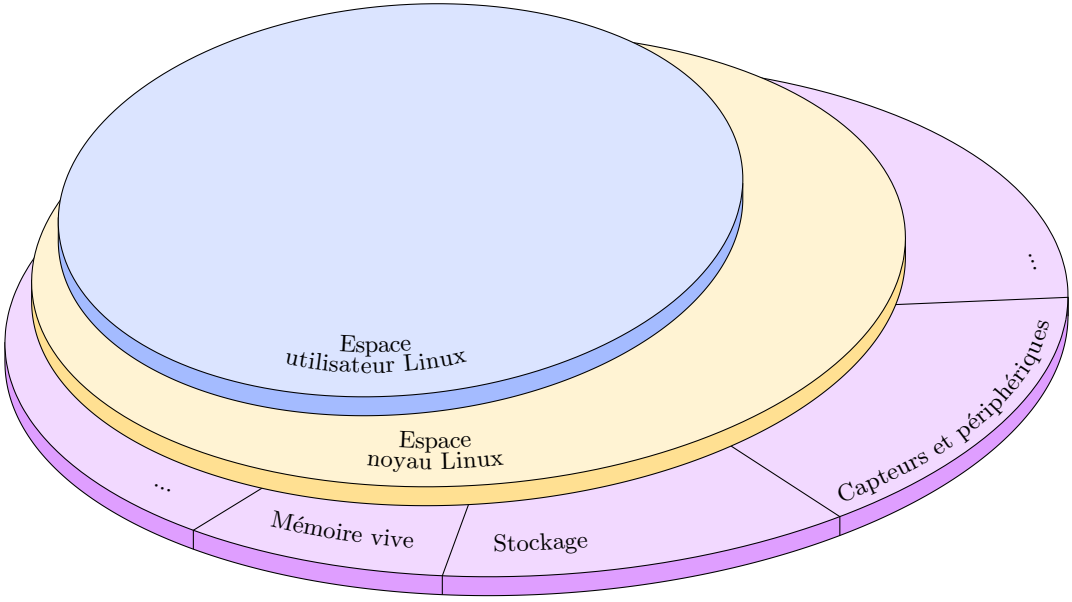
- Applications dangereuses pour le système
- Applications dangereuses pour l'utilisateur

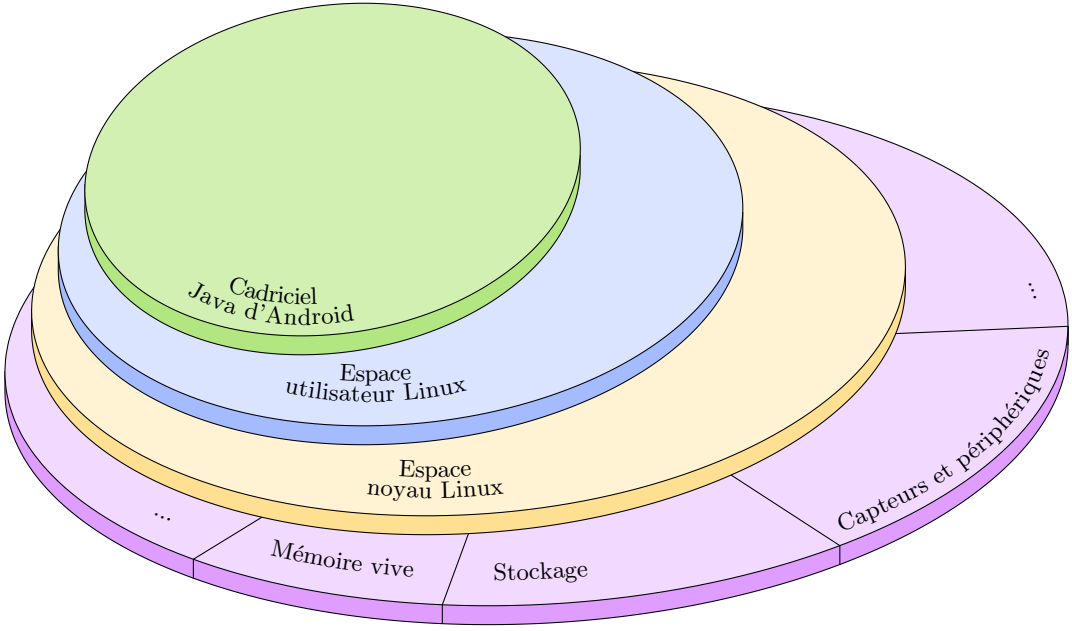
- Applications dangereuses pour le système
- Applications dangereuses pour l'utilisateur
- Applications jugées indésirables selon des critères moraux ou sociétaux

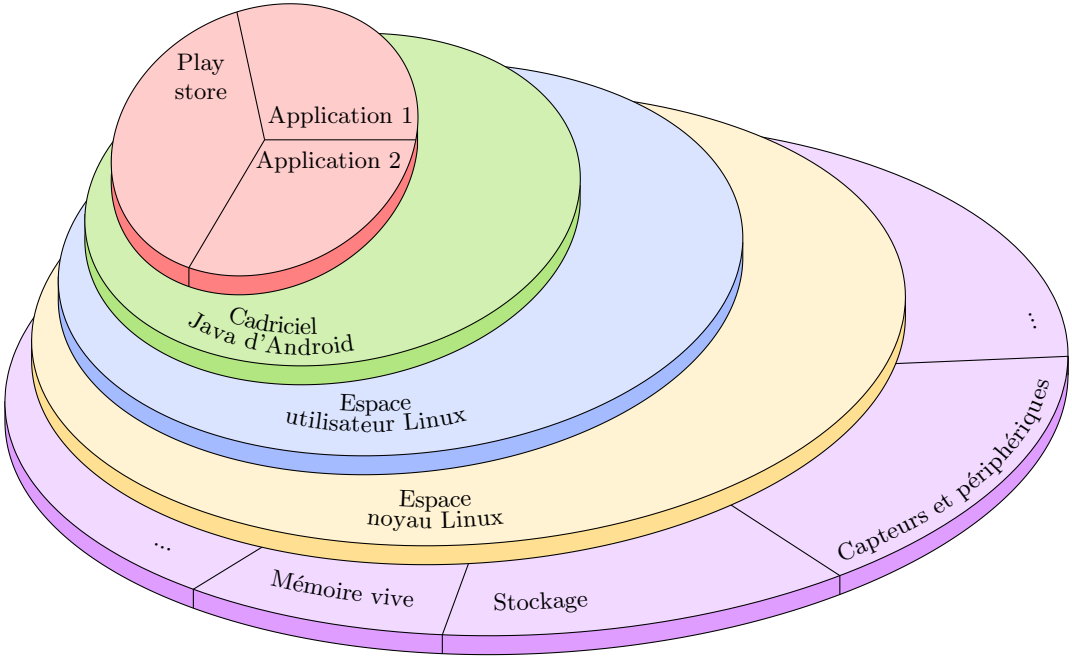
- Applications dangereuses pour le système
- Applications dangereuses pour l'utilisateur
- Applications jugées indésirables selon des critères moraux ou sociétaux

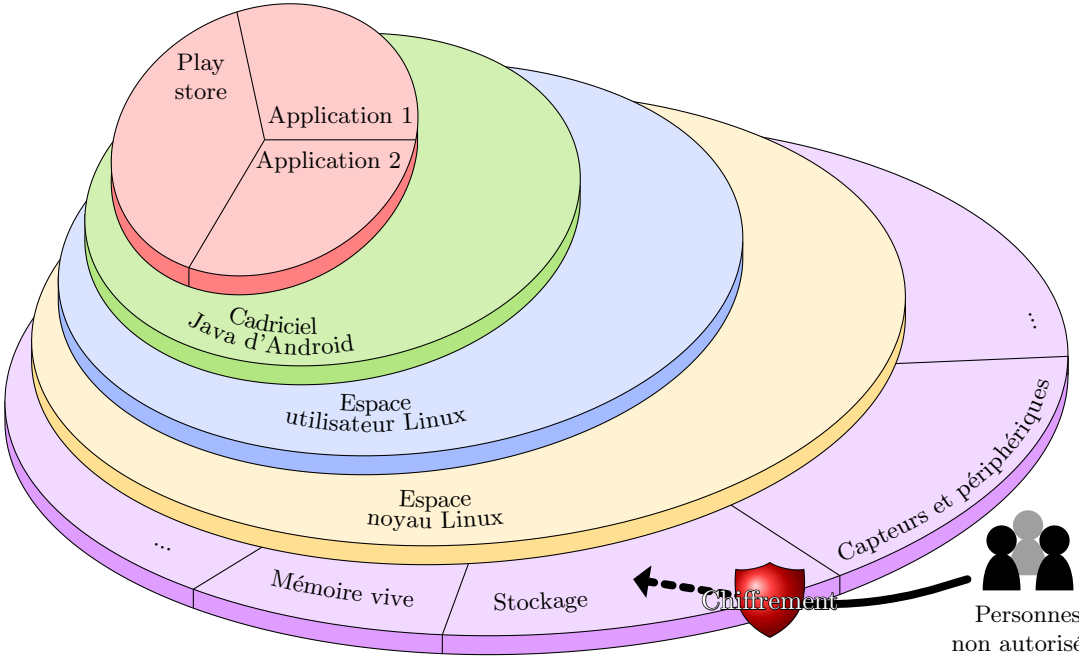

...
Mémoire vive
Stockage
Capteurs et périphériques
...

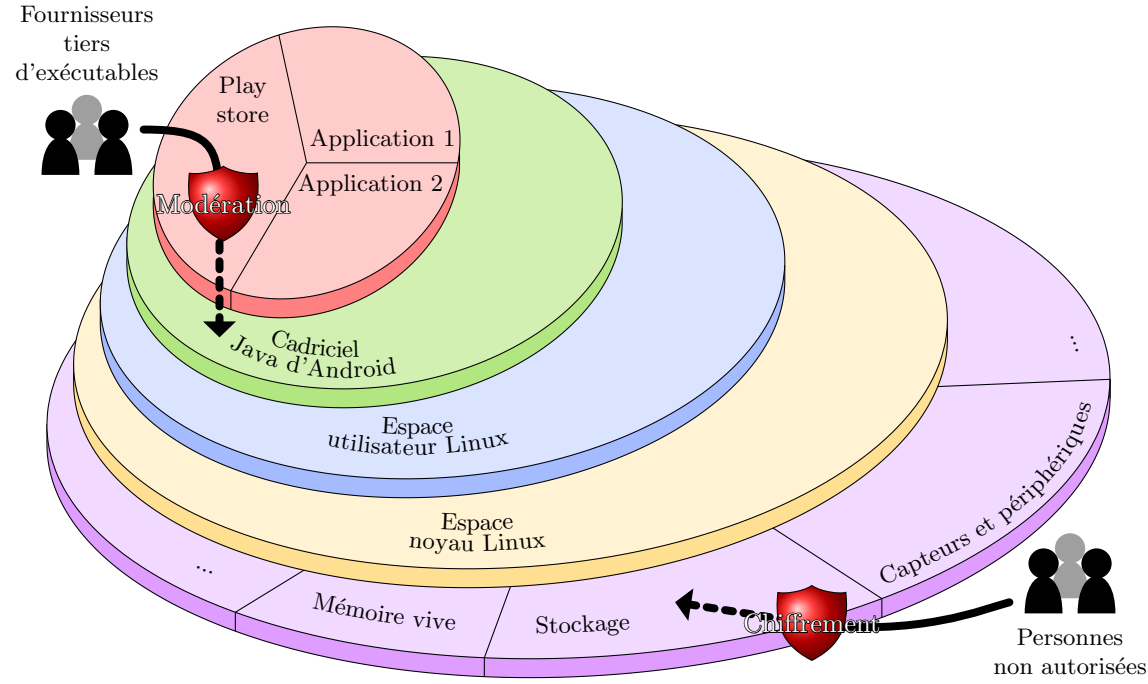

Espace
noyau Linux
...
Mémoire vive
Stockage
Capteurs et périphériques
...

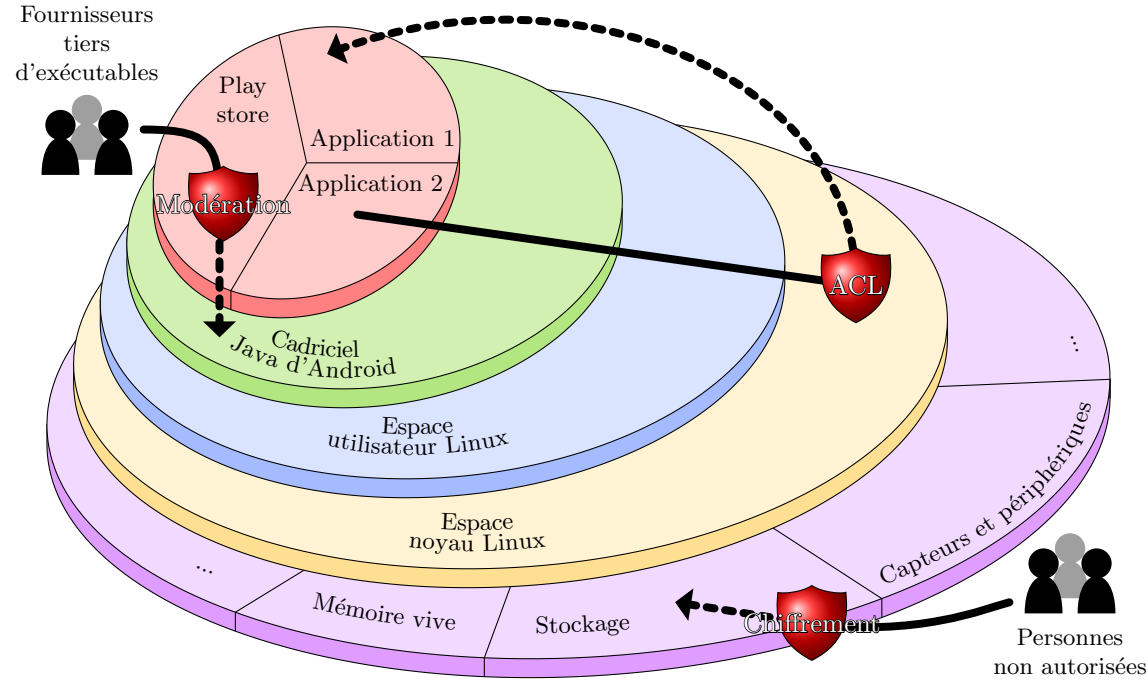

Espace
utilisateur Linux
Espace
noyau Linux
...
Mémoire vive
Stockage
Capteurs et périphériques
...

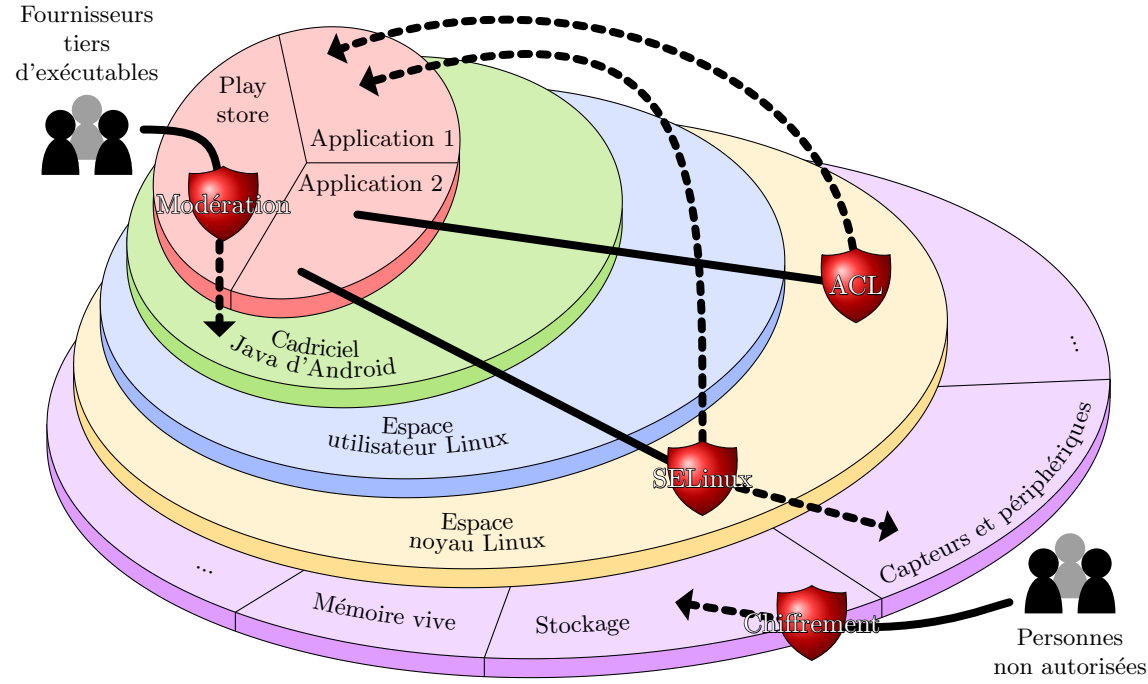

Cadriciel
Java d'Android
Espace
utilisateur Linux
Espace
noyau Linux
...
Mémoire vive
Stockage
Capteurs et périphériques
...

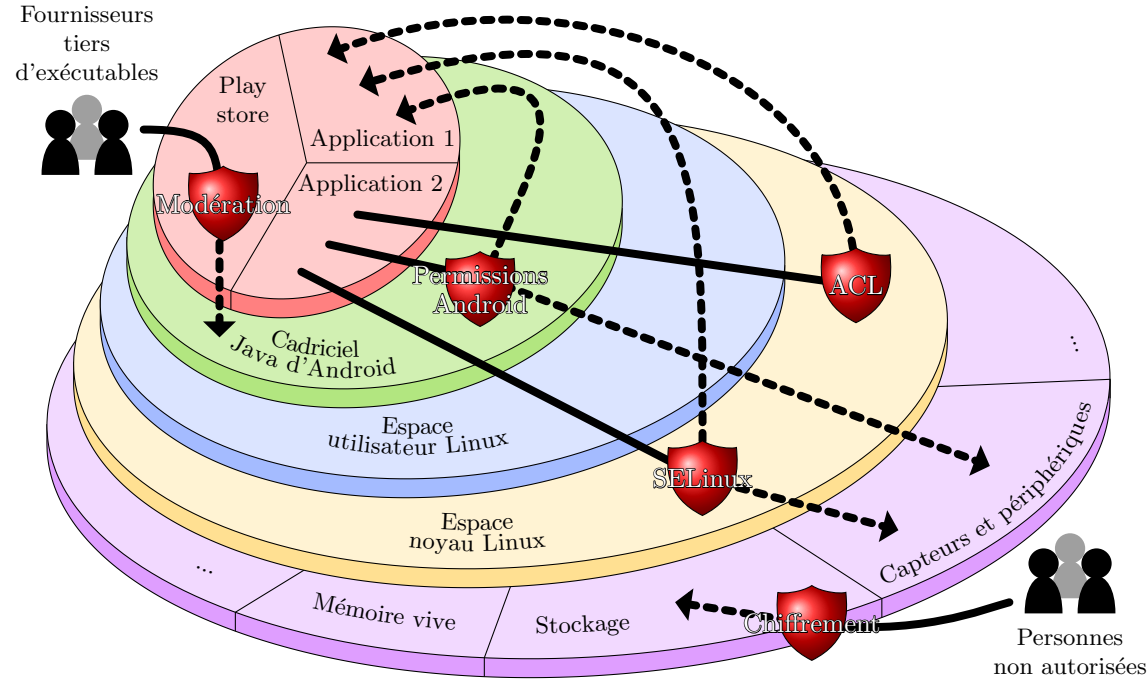

Play
store
Application 1
Application 2
Cadriciel
Java d'Android
Espace
utilisateur Linux
Espace
noyau Linux
...
Mémoire vive
Stockage
Capteurs et périphériques
...


Play
store
Application 1
Application 2
Cadriciel
Java d'Android
Espace
utilisateur Linux
Espace
noyau Linux
...
Mémoire vive
Stockage
Chiffrement
Capteurs et périphériques
...
Personnes
non autorisées


Fournisseurs tiers d'exécutables
Play store
Application 1
Application 2
Modération
Cadriciel Java d'Android
Espace utilisateur Linux
Espace noyau Linux
...
Mémoire vive
Stockage
Chiffrement
Capteurs et périphériques
...
Personnes non autorisées


Fournisseurs tiers d'exécutables
Play store
Application 1
Application 2
Modération
ACL
Cadriciel Java d'Android
Espace utilisateur Linux
Espace noyau Linux
...
Capteurs et périphériques
...
Mémoire vive
Stockage
Chiffrement
Personnes non autorisées


Fournisseurs tiers d'exécutables
Play store
Application 1
Application 2
Modération
ACL
Cadriciel Java d'Android
Espace utilisateur Linux
SELinux
Espace noyau Linux
...
Capteurs et périphériques
...
Mémoire vive
Stockage
Chiffrement
Personnes non autorisées


Fournisseurs tiers d'exécutables
Play store
Application 1
Application 2
Modération
Permissions Android
ACL
Cadriciel Java d'Android
Espace utilisateur Linux
SELinux
Espace noyau Linux
Capteurs et périphériques
...
...
Mémoire vive
Stockage
Chiffrement
Personnes non autorisées

Contributions

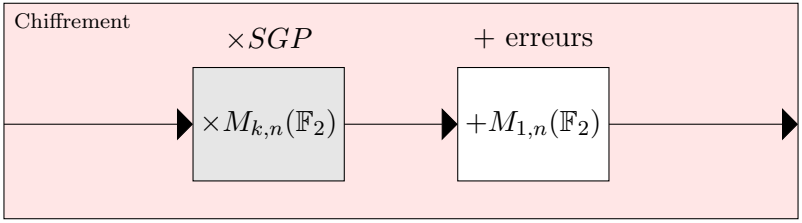
Cryptosystème de McEliece en environnement ouvert

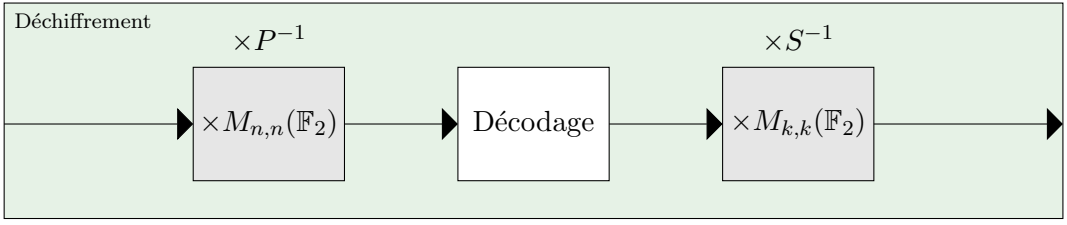
Journée thématique sur les Attaques par Injection de Fautes (JAIF) 2022 :
L'attaque en faute : la bête noire des boîtes blanches

Security of Software/Hardware Interfaces (SILM) 2023 au sein d'*European Symposium on Security and Privacy* (EuroS&P) :
Faulting original McEliece's implementations is possible — How to mitigate this risk ?

Brevet numéro WO2024083855, date de priorité au 17 octobre 2022 :
Clés cryptographiques en boîte blanche

[McE78]


Chiffrement
$\times SGP$
$+$ erreurs
$\times M_{k,n}(\mathbb{F}_2)$
$+M_{1,n}(\mathbb{F}_2)$


Déchiffrement
$\times P^{-1}$
$\times S^{-1}$
$\times M_{n,n}(\mathbb{F}_2)$
Décodage
$\times M_{k,k}(\mathbb{F}_2)$

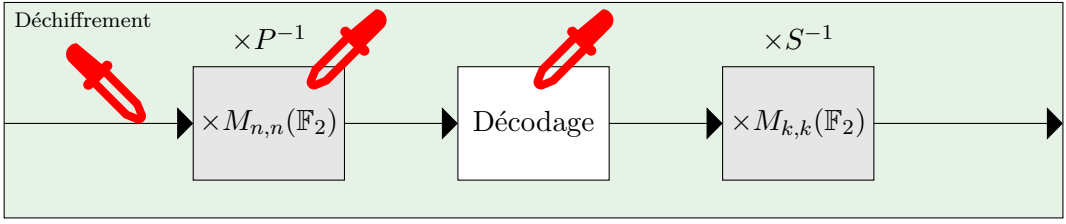
- Codes de Goppa

- Codes de Goppa
- Codes de Reed-Solomon généralisés
- Codes de Reed-Muller
- Codes géométriques algébriques
- Codes Bose-Chaudhuri-Hocquenghem
- Codes alternants quasi-cycliques et alternants quasi-dyadiques
- Codes sur $\mathbb{F}_q$

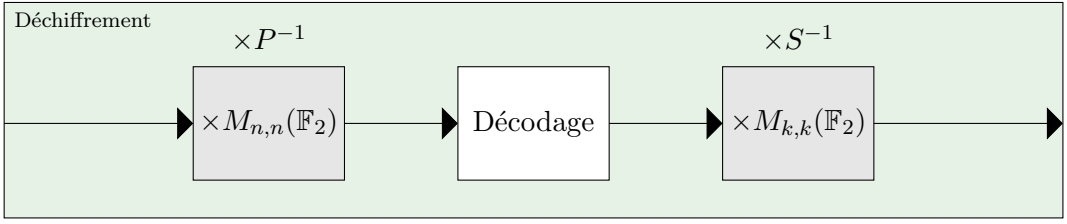
- Codes de Goppa
- ~~Codes de Reed-Solomon généralisés~~ [SS92]
- ~~Codes de Reed-Muller~~ [MS07]
- ~~Codes géométriques algébriques~~ [FM08 ; CMP14]
- ~~Codes Bose-Chaudhuri-Hocquenghem~~ [OTD10]
- ~~Codes alternants quasi-cycliques et alternants quasi-dyadiques~~ [Fau+10]
- ~~Codes sur $\mathbb{F}_q$~~ [COT17]

- Codes de Goppa
- ~~Codes de Reed-Solomon généralisés~~ [SS92]
- ~~Codes de Reed-Muller~~ [MS07]
- ~~Codes géométriques algébriques~~ [FM08 ; CMP14]
- ~~Codes Bose-Chaudhuri-Hocquenghem~~ [OTD10]
- ~~Codes alternants quasi-cycliques et alternants quasi-dyadiques~~ [Fau+10]
- ~~Codes sur $\mathbb{F}_q$~~ [COT17]

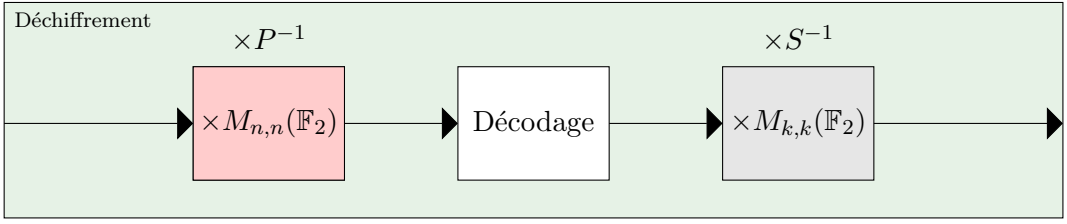
[Sho+10 ; Str11a ; Str+08 ; Str10 ; Ava+10 ; Str11b ; Mol+11 ; Che+14 ; VG14 ; HMP10]



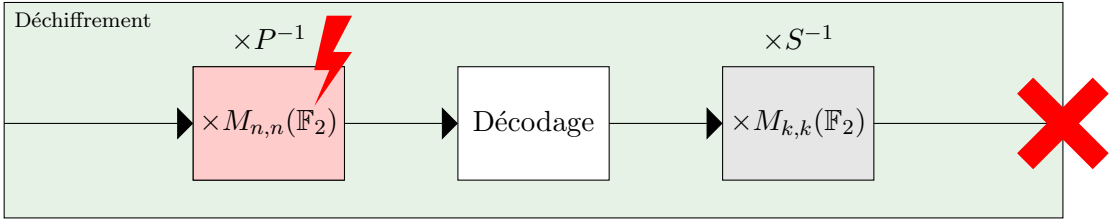
- Matrice de permutation P
- Code correcteur
- Matrice de mélange S



- Matrice de permutation P
- Code correcteur
- Matrice de mélange S

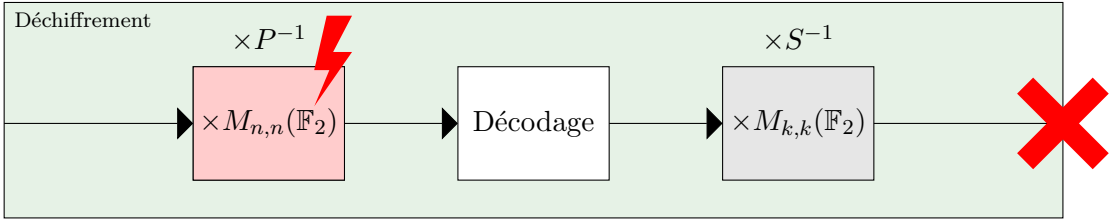


- Matrice de permutation P
- Code correcteur
- Matrice de mélange S



- Matrice de permutation P
- Code correcteur
- Matrice de mélange S

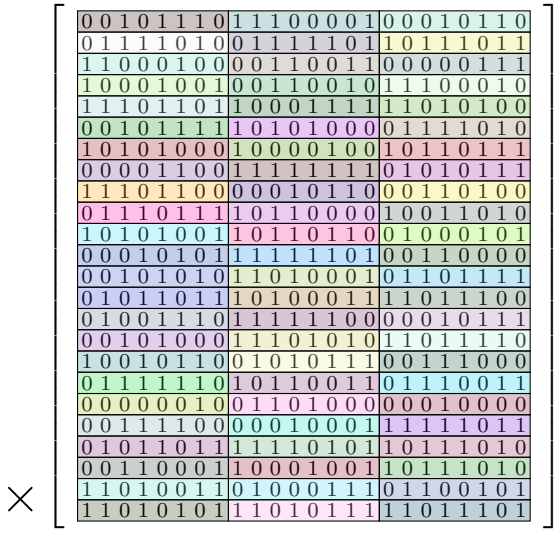
$$\begin{bmatrix}
0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\
0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0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

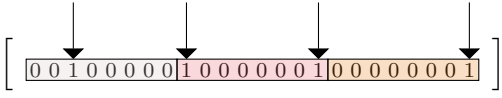


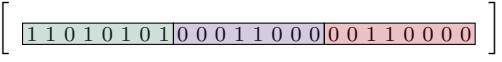
$$\times \begin{bmatrix}
0&0&1&0&1&1&1&0&1&1&1&0&0&0&0&1&0&0&0&1&0&1&1&0\\
0&1&1&1&1&0&1&0&0&1&1&1&1&1&1&0&1&1&0&1&1&1&0&1&1\\
1&1&0&0&0&1&0&0&0&0&1&1&0&0&1&1&0&0&0&0&0&1&1&1\\
1&0&0&0&1&0&0&1&0&0&1&1&0&0&1&0&1&1&1&0&0&0&1&0\\
1&1&1&0&1&1&0&1&1&0&0&0&1&1&1&1&1&1&0&1&0&1&0&0\\
0&0&1&0&1&1&1&1&1&0&1&0&1&0&0&0&0&1&1&1&1&0&1&0\\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

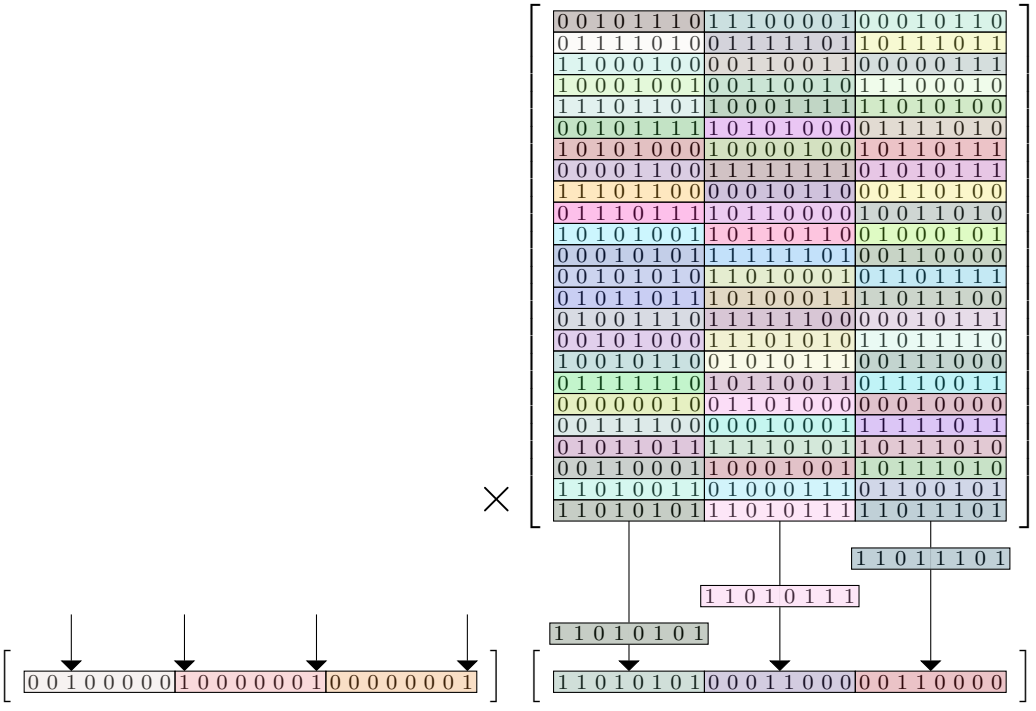
$$\begin{bmatrix} 0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1 \end{bmatrix} \quad \begin{bmatrix} 1&1&0&1&0&1&0&1&0&0&0&1&1&0&0&0&0&0&1&1&0&0&0&0 \end{bmatrix}$$

$$\begin{bmatrix} 0\,0\,1\,0\,0\,0\,0\,0 & 1\,0\,0\,0\,0\,0\,0\,1 & 0\,0\,0\,0\,0\,0\,0\,1 \end{bmatrix} \times \begin{bmatrix} 0\,0\,1\,0\,1\,1\,1\,0 & 1\,1\,1\,0\,0\,0\,0\,1 & 0\,0\,0\,1\,0\,1\,1\,0 \\ 0\,1\,1\,1\,1\,0\,1\,0 & 0\,1\,1\,1\,1\,1\,0\,1 & 1\,0\,1\,1\,1\,0\,1\,1 \\ 1\,1\,0\,0\,0\,1\,0\,0 & 0\,0\,1\,1\,0\,0\,1\,1 & 0\,0\,0\,0\,0\,1\,1\,1 \\ 1\,0\,0\,0\,1\,0\,0\,1 & 0\,0\,1\,1\,0\,0\,1\,0 & 1\,1\,1\,0\,0\,0\,1\,0 \\ 1\,1\,1\,0\,1\,1\,0\,1 & 1\,0\,0\,0\,1\,1\,1\,1 & 1\,1\,0\,1\,0\,1\,0\,0 \\ 0\,0\,1\,0\,1\,1\,1\,1 & 1\,0\,1\,0\,1\,0\,0\,0 & 0\,1\,1\,1\,1\,0\,1\,0 \\ 1\,0\,1\,0\,1\,0\,0\,0 & 1\,0\,0\,0\,0\,1\,0\,0 & 1\,0\,1\,1\,0\,1\,1\,1 \\ 0\,0\,0\,0\,1\,1\,0\,0 & 1\,1\,1\,1\,1\,1\,1\,1 & 0\,1\,0\,1\,0\,1\,1\,1 \\ 1\,1\,1\,0\,1\,1\,0\,0 & 0\,0\,0\,1\,0\,1\,1\,0 & 0\,0\,1\,1\,0\,1\,0\,0 \\ 0\,1\,1\,1\,0\,1\,1\,1 & 1\,0\,1\,1\,0\,0\,0\,0 & 1\,0\,0\,1\,1\,0\,1\,0 \\ 1\,0\,1\,0\,1\,0\,0\,1 & 1\,0\,1\,1\,0\,1\,1\,0 & 0\,1\,0\,0\,0\,1\,0\,1 \\ 0\,0\,0\,1\,0\,1\,0\,1 & 1\,1\,1\,1\,1\,1\,0\,1 & 0\,0\,1\,1\,0\,0\,0\,0 \\ 0\,0\,1\,0\,1\,0\,1\,0 & 1\,1\,0\,1\,0\,0\,0\,1 & 0\,1\,1\,0\,1\,1\,1\,1 \\ 0\,1\,0\,1\,1\,0\,1\,1 & 1\,0\,1\,0\,0\,0\,1\,1 & 1\,1\,0\,1\,1\,1\,0\,0 \\ 0\,1\,0\,0\,1\,1\,1\,0 & 1\,1\,1\,1\,1\,1\,0\,0 & 0\,0\,0\,1\,0\,1\,1\,1 \\ 0\,0\,1\,0\,1\,0\,0\,0 & 1\,1\,1\,0\,1\,0\,1\,0 & 1\,1\,0\,1\,1\,1\,1\,0 \\ 1\,0\,0\,1\,0\,1\,1\,0 & 0\,1\,0\,1\,0\,1\,1\,1 & 0\,0\,1\,1\,1\,0\,0\,0 \\ 0\,1\,1\,1\,1\,1\,1\,0 & 1\,0\,1\,1\,0\,0\,1\,1 & 0\,1\,1\,1\,0\,0\,1\,1 \\ 0\,0\,0\,0\,0\,0\,1\,0 & 0\,1\,1\,0\,1\,0\,0\,0 & 0\,0\,0\,1\,0\,0\,0\,0 \\ 0\,0\,1\,1\,1\,1\,0\,0 & 0\,0\,0\,1\,0\,0\,0\,1 & 1\,1\,1\,1\,1\,0\,1\,1 \\ 0\,1\,0\,1\,1\,0\,1\,1 & 1\,1\,1\,1\,0\,1\,0\,1 & 1\,0\,1\,1\,1\,0\,1\,0 \\ 0\,0\,1\,1\,0\,0\,0\,1 & 1\,0\,0\,0\,1\,0\,0\,1 & 1\,0\,1\,1\,1\,0\,1\,0 \\ 1\,1\,0\,1\,0\,0\,1\,1 & 0\,1\,0\,0\,0\,1\,1\,1 & 0\,1\,1\,0\,0\,1\,0\,1 \\ 1\,1\,0\,1\,0\,1\,0\,1 & 1\,1\,0\,1\,0\,1\,1\,1 & 1\,1\,0\,1\,1\,1\,0\,1 \end{bmatrix} = \begin{bmatrix} 1\,1\,0\,1\,0\,1\,0\,1 & 0\,0\,0\,1\,1\,0\,0\,0 & 0\,0\,1\,1\,0\,0\,0\,0 \end{bmatrix}$$


0 0 1 0 1 1 1 0 | 1 1 1 0 0 0 0 1 | 0 0 0 1 0 1 1 0
0 1 1 1 1 0 1 0 | 0 1 1 1 1 1 0 1 | 1 0 1 1 1 0 1 1
1 1 0 0 0 1 0 0 | 0 0 1 1 0 0 1 1 | 0 0 0 0 0 1 1 1
1 0 0 0 1 0 0 1 | 0 0 1 1 0 0 1 0 | 1 1 1 0 0 0 1 0
1 1 1 0 1 1 0 1 | 1 0 0 0 1 1 1 1 | 1 1 0 1 0 1 0 0
0 0 1 0 1 1 1 1 | 1 0 1 0 1 0 0 0 | 0 1 1 1 1 0 1 0
1 0 1 0 1 0 0 0 | 1 0 0 0 0 1 0 0 | 1 0 1 1 0 1 1 1
0 0 0 0 1 1 0 0 | 1 1 1 1 1 1 1 1 | 0 1 0 1 0 1 1 1
1 1 1 0 1 1 0 0 | 0 0 0 1 0 1 1 0 | 0 0 1 1 0 1 0 0
0 1 1 1 0 1 1 1 | 1 0 1 1 0 0 0 0 | 1 0 0 1 1 0 1 0
1 0 1 0 1 0 0 1 | 1 0 1 1 0 1 1 0 | 0 1 0 0 0 1 0 1
0 0 0 1 0 1 0 1 | 1 1 1 1 1 1 0 1 | 0 0 1 1 0 0 0 0
0 0 1 0 1 0 1 0 | 1 1 0 1 0 0 0 1 | 0 1 1 0 1 1 1 1
0 1 0 1 1 0 1 1 | 1 0 1 0 0 0 1 1 | 1 1 0 1 1 1 0 0
0 1 0 0 1 1 1 0 | 1 1 1 1 1 1 0 0 | 0 0 0 1 0 1 1 1
0 0 1 0 1 0 0 0 | 1 1 1 0 1 0 1 0 | 1 1 0 1 1 1 1 0
1 0 0 1 0 1 1 0 | 0 1 0 1 0 1 1 1 | 0 0 1 1 1 0 0 0
0 1 1 1 1 1 1 0 | 1 0 1 1 0 0 1 1 | 0 1 1 1 0 0 1 1
0 0 0 0 0 0 1 0 | 0 1 1 0 1 0 0 0 | 0 0 0 1 0 0 0 0
0 0 1 1 1 1 0 0 | 0 0 0 1 0 0 0 1 | 1 1 1 1 1 0 1 1
0 1 0 1 1 0 1 1 | 1 1 1 1 0 1 0 1 | 1 0 1 1 1 0 1 0
0 0 1 1 0 0 0 1 | 1 0 0 0 1 0 0 1 | 1 0 1 1 1 0 1 0
1 1 0 1 0 0 1 1 | 0 1 0 0 0 1 1 1 | 0 1 1 0 0 1 0 1
1 1 0 1 0 1 0 1 | 1 1 0 1 0 1 1 1 | 1 1 0 1 1 1 0 1


0 0 1 0 0 0 0 0 | 1 0 0 0 0 0 0 1 | 0 0 0 0 0 0 0 1


1 1 0 1 0 1 0 1 | 0 0 0 1 1 0 0 0 | 0 0 1 1 0 0 0 0


0 0 1 0 1 1 1 0 | 1 1 1 0 0 0 0 1 | 0 0 0 1 0 1 1 0
0 1 1 1 1 0 1 0 | 0 1 1 1 1 1 0 1 | 1 0 1 1 1 0 1 1
1 1 0 0 0 1 0 0 | 0 0 1 1 0 0 1 1 | 0 0 0 0 0 1 1 1
1 0 0 0 1 0 0 1 | 0 0 1 1 0 0 1 0 | 1 1 1 0 0 0 1 0
1 1 1 0 1 1 0 1 | 1 0 0 0 1 1 1 1 | 1 1 0 1 0 1 0 0
0 0 1 0 1 1 1 1 | 1 0 1 0 1 0 0 0 | 0 1 1 1 1 0 1 0
1 0 1 0 1 0 0 0 | 1 0 0 0 0 1 0 0 | 1 0 1 1 0 1 1 1
0 0 0 0 1 1 0 0 | 1 1 1 1 1 1 1 1 | 0 1 0 1 0 1 1 1
1 1 1 0 1 1 0 0 | 0 0 0 1 0 1 1 0 | 0 0 1 1 0 1 0 0
0 1 1 1 0 1 1 1 | 1 0 1 1 0 0 0 0 | 1 0 0 1 1 0 1 0
1 0 1 0 1 0 0 1 | 1 0 1 1 0 1 1 0 | 0 1 0 0 0 1 0 1
0 0 0 1 0 1 0 1 | 1 1 1 1 1 1 0 1 | 0 0 1 1 0 0 0 0
0 0 1 0 1 0 1 0 | 1 1 0 1 0 0 0 1 | 0 1 1 0 1 1 1 1
0 1 0 1 1 0 1 1 | 1 0 1 0 0 0 1 1 | 1 1 0 1 1 1 0 0
0 1 0 0 1 1 1 0 | 1 1 1 1 1 1 0 0 | 0 0 0 1 0 1 1 1
0 0 1 0 1 0 0 0 | 1 1 1 0 1 0 1 0 | 1 1 0 1 1 1 1 0
1 0 0 1 0 1 1 0 | 0 1 0 1 0 1 1 1 | 0 0 1 1 1 0 0 0
0 1 1 1 1 1 1 0 | 1 0 1 1 0 0 1 1 | 0 1 1 1 0 0 1 1
0 0 0 0 0 0 1 0 | 0 1 1 0 1 0 0 0 | 0 0 0 1 0 0 0 0
0 0 1 1 1 1 0 0 | 0 0 0 1 0 0 0 1 | 1 1 1 1 1 0 1 1
0 1 0 1 1 0 1 1 | 1 1 1 1 0 1 0 1 | 1 0 1 1 1 0 1 0
0 0 1 1 0 0 0 1 | 1 0 0 0 1 0 0 1 | 1 0 1 1 1 0 1 0
1 1 0 1 0 0 1 1 | 0 1 0 0 0 1 1 1 | 0 1 1 0 0 1 0 1
1 1 0 1 0 1 0 1 | 1 1 0 1 0 1 1 1 | 1 1 0 1 1 1 0 1
1 1 0 1 1 1 0 1
1 1 0 1 0 1 1 1
1 1 0 1 0 1 0 1
0 0 1 0 0 0 0 0 | 1 0 0 0 0 0 0 1 | 0 0 0 0 0 0 0 1
1 1 0 1 0 1 0 1 | 0 0 0 1 1 0 0 0 | 0 0 1 1 0 0 0 0

Soit x un vecteur utilisé en entrée du chiffrement f d'une implémentation de McEliece basée sur un nombre maximal d'erreurs t. Alors si w est le calcul du poids de Hamming :

$$w(f(x)) \leq t \Rightarrow w(x) = 0 \Leftrightarrow x = 0$$

Mnémonique	Code	Description
AND	0000	Rd = Rn AND opérande 2
EOR	0001	Rd = Rn EOR opérande 2
SUB	0010	Rd = Rn - opérande 2
RSB	0011	Rd = opérande 2 - Rn
ADD	0100	Rd = Rn + opérande 2
ADC	0101	Rd = Rn + opérande 2 + C
SBC	0110	Rd = Rn - opérande 2 + C
RSC	0111	Rd = opérande 2 - Rn + C
TST	1000	régler codes de condition selon Rn AND opérande 2
TEQ	1001	régler codes de condition selon Rn EOR opérande 2
CMP	1010	régler codes de condition selon Rn - opérande 2
CMN	1011	régler codes de condition selon Rn + opérande 2
ORR	1100	Rd = Rn OR opérande 2
MOV	1101	Rd = opérande 2
BIC	1110	Rd = Rn AND NOT opérande 2
MVN	1111	Rd = NOT opérande 2

Mnémonique	Code	Description
AND	0000	Rd = Rn AND opérande 2
EOR	0001	Rd = Rn EOR opérande 2
SUB	0010	Rd = Rn - opérande 2
RSB	0011	Rd = opérande 2 - Rn
ADD	0100	Rd = Rn + opérande 2
ADC	0101	Rd = Rn + opérande 2 + C
SBC	0110	Rd = Rn - opérande 2 + C
RSC	0111	Rd = opérande 2 - Rn + C
TST	1000	régler codes de condition selon Rn AND opérande 2
TEQ	1001	régler codes de condition selon Rn EOR opérande 2
CMP	1010	régler codes de condition selon Rn - opérande 2
CMN	1011	régler codes de condition selon Rn + opérande 2
ORR	1100	Rd = Rn OR opérande 2
MOV	1101	Rd = opérande 2
BIC	1110	Rd = Rn AND NOT opérande 2
MVN	1111	Rd = NOT opérande 2

Mnémonique	Code	Description
AND	0000	Rd = Rn AND opérande 2
EOR	0001	Rd = Rn EOR opérande 2
SUB	0010	Rd = Rn - opérande 2
RSB	0011	Rd = opérande 2 - Rn
ADD	0100	Rd = Rn + opérande 2
ADC	0101	Rd = Rn + opérande 2 + C
SBC	0110	Rd = Rn - opérande 2 + C
RSC	0111	Rd = opérande 2 - Rn + C
TST	1000	régler codes de condition selon Rn AND opérande 2
TEQ	1001	régler codes de condition selon Rn EOR opérande 2
CMP	1010	régler codes de condition selon Rn - opérande 2
CMN	1011	régler codes de condition selon Rn + opérande 2
ORR	1100	Rd = Rn OR opérande 2
MOV	1101	Rd = opérande 2
BIC	1110	Rd = Rn AND NOT opérande 2
MVN	1111	Rd = NOT opérande 2

$$\left[\begin{array}{ccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \end{array}\right]$$

$$n = 9$$

$$p = 3$$

$$t = 4$$

$$\left[\begin{array}{ccc|ccc|ccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\
\mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\
0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0
\end{array}\right]$$

$$n = 9$$

$$p = 3$$

$$t = 4$$

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

$$\times$$

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

Les lignes 2, 3 et 6 ont forcément leurs uns respectifs dans des groupes de colonnes différents

$$\begin{bmatrix} 0\,1\,1\,0\,0\,1\,0\,0\,0 \end{bmatrix} \times \begin{bmatrix} 0\,0\,0\,0\,0\,0\,0\,1\,0 \\ 1\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1 \\ 0\,1\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,1\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,1\,0\,0 \end{bmatrix} = \begin{bmatrix} 1\,0\,0\,1\,0\,0\,1\,1\,1 \end{bmatrix}$$

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

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

Les lignes 4, 8 et 9 ont forcément leurs uns respectifs dans des groupes de colonnes différents

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

$$\times$$

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

$$\begin{bmatrix} 0&0&0&0&0&0&0&1&1&0 \end{bmatrix} \times \begin{bmatrix} 0&0&0&0&0&0&0&1&0 \\ 1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1 \\ 0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&1&0&0 \end{bmatrix} = \begin{bmatrix} 1&1&1&1&0&0&1&0&0 \end{bmatrix}$$

Les lignes 6, 7 et 9 ont forcément leurs uns respectifs dans des groupes de colonnes différents

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

$$\times$$

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

$$\begin{bmatrix} 1\,0\,0\,0\,0\,0\,1\,1\,0 \end{bmatrix} \times \begin{bmatrix} 0\,0\,0\,0\,0\,0\,0\,1\,0 \\ 1\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1 \\ 0\,1\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,1\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,1\,0\,0 \end{bmatrix} = \begin{bmatrix} 1\,1\,1\,0\,0\,1\,0\,1\,0 \end{bmatrix}$$

Les lignes 1, 7 et 8 ont forcément leurs uns respectifs dans des groupes de colonnes différents

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

$$\times$$

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

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

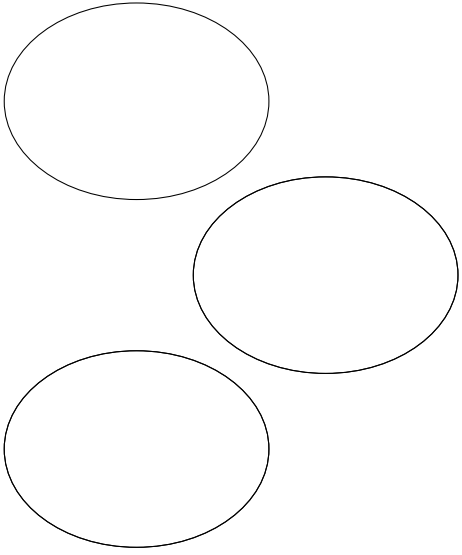
$$\begin{bmatrix} 0&1&0&0&0&0&0&1&1 \end{bmatrix} \begin{bmatrix} 1&0&0&1&1&1&1&0&0 \end{bmatrix}$$

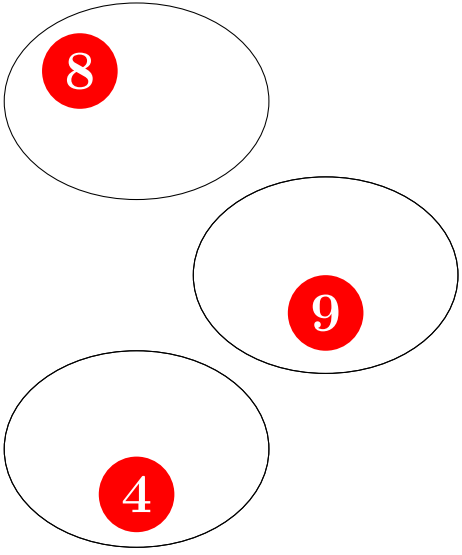
Les lignes 2, 8 et 9 ont forcément leurs uns respectifs dans des groupes de colonnes différents

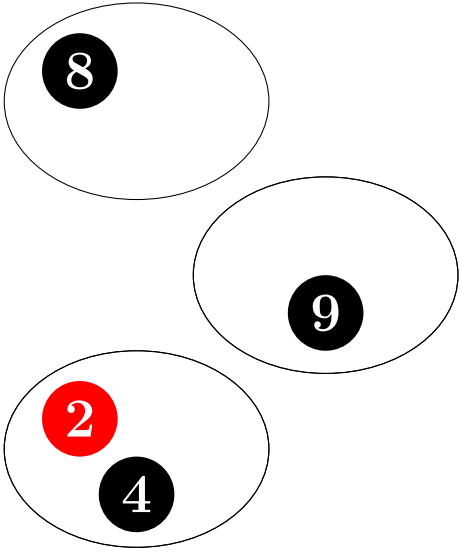
$$\begin{bmatrix} 0&0&0&0&0&0&0&1&0 \\ 1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1 \\ 0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&1&0&0 \end{bmatrix}$$

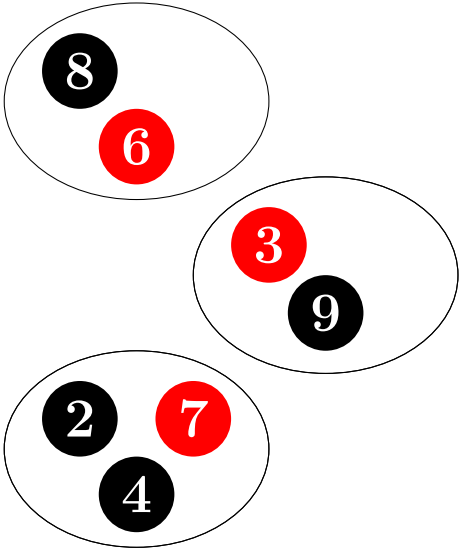
$$\times$$

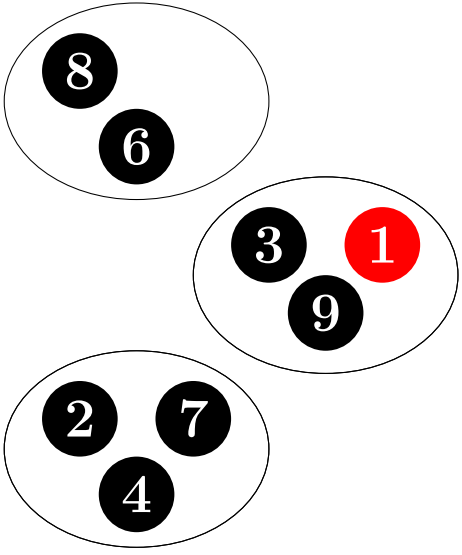
$$\begin{bmatrix} 0&1&0&0&0&0&0&1&1 \end{bmatrix} \begin{bmatrix} 1&0&0&1&1&1&1&0&0 \end{bmatrix}$$

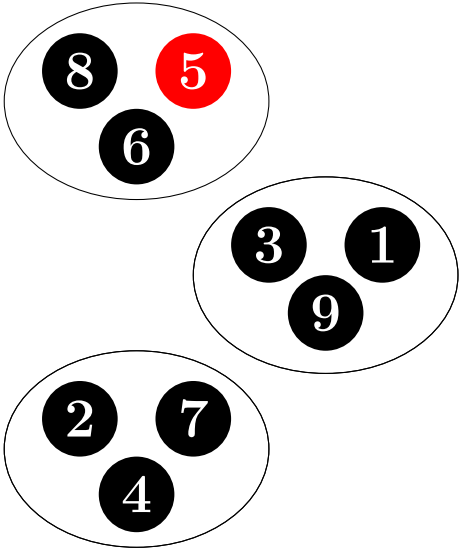


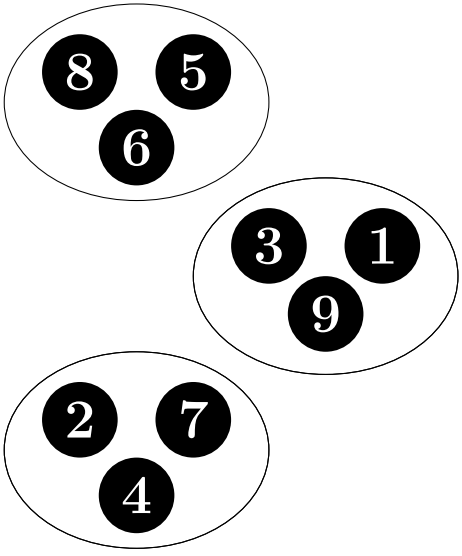

8
9
4


8
9
2
4

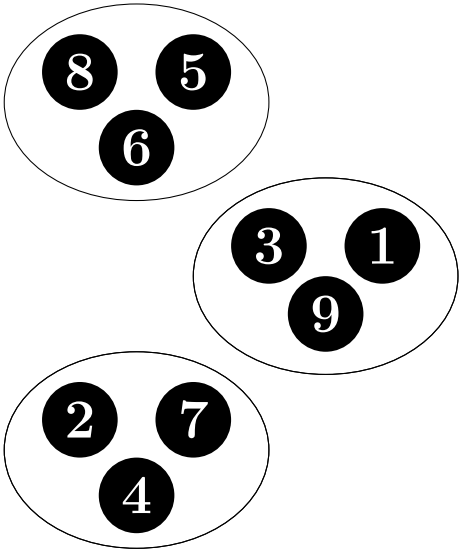

8
6
3
9
2
7
4


8
6
3
1
9
2
7
4

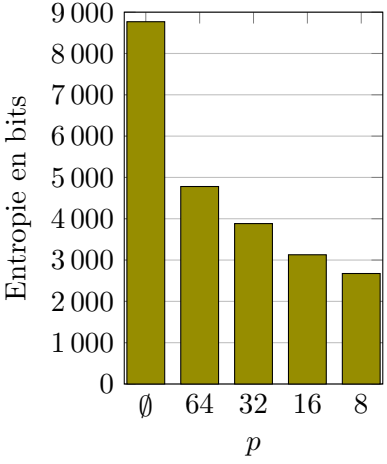

8
5
6
3
1
9
2
7
4



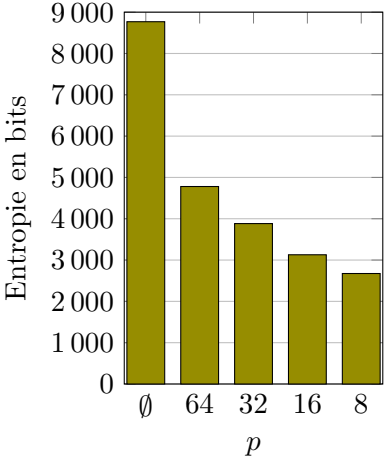
$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 &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



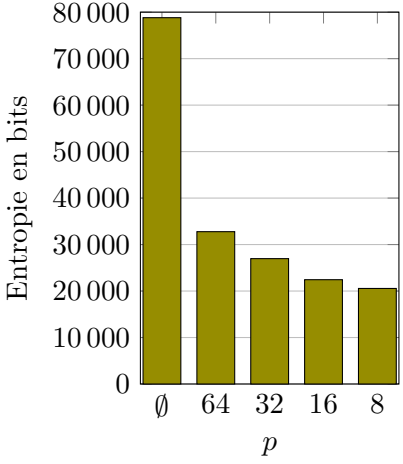
$$\left[\begin{array}{ccc|ccc|ccc}
0&0&0&0&0&0&0&1&0\\
1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1\\
0&1&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0\\
0&0&0&1&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&1&0&0
\end{array}\right]$$


9 000
8 000
7 000
6 000
5 000
4 000
3 000
2 000
1 000
0
Entropie en bits
∅
64
32
16
8
p

$n = 1\ 024$


Entropie en bits
9 000
8 000
7 000
6 000
5 000
4 000
3 000
2 000
1 000
0
∅
64
32
16
8
p

$n = 1\ 024$


Entropie en bits
80 000
70 000
60 000
50 000
40 000
30 000
20 000
10 000
0
∅
64
32
16
8
p

$n = 6\ 960$

~~Autoprotection de ses propres exécutables~~

~~Autoprotection de ses propres exécutables~~

Bénéficier des garanties du système d'exploitation

Contributions

Isolation des applications sur Android

Symposium sur la Sécurité des Technologies de l'Information et des Communications (SSTIC) 2023 :
Batterie à bord, quand les jauges de carburant dépassent les limites

International Workshop on Security (IWSEC) 2023 :
Power analysis pushed too far — Breaking Android-based isolation with fuel gauges
Publication associée dans *Lecture Notes in Computer Science* (LNCS), volume 14128

Brevet numéro WO2024121142, date de priorité au 6 décembre 2022 :
Procédé de protection d'un terminal contre une attaque par canal auxiliaire

- Autonomie de la batterie plus longue

- Autonomie de la batterie plus longue
- Durée de vie de la batterie plus longue

- Autonomie de la batterie plus longue
- Durée de vie de la batterie plus longue
- Température de fonctionnement moins élevée

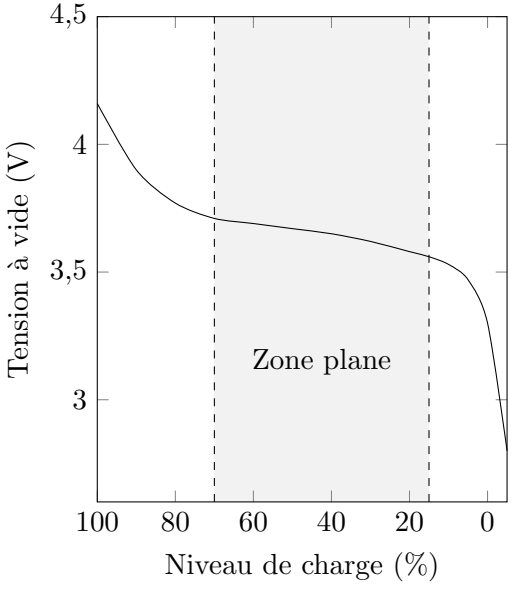
- Autonomie de la batterie plus longue
- Durée de vie de la batterie plus longue
- Température de fonctionnement moins élevée
- Durée de charge plus courte

- Autonomie de la batterie plus longue
- Durée de vie de la batterie plus longue
- Température de fonctionnement moins élevée
- Durée de charge plus courte
- Réduction des risques

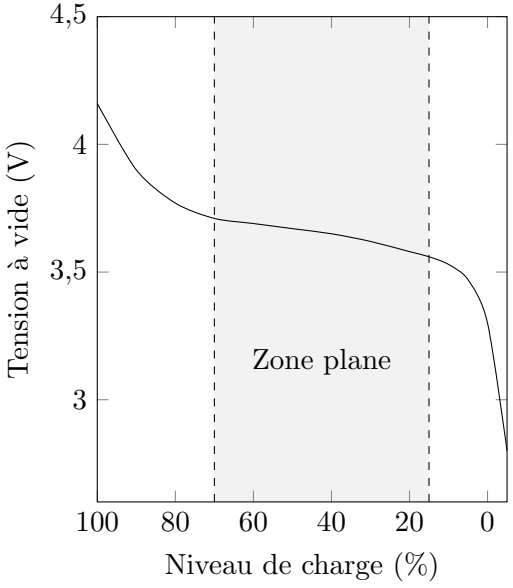
- Autonomie de la batterie plus longue
- Durée de vie de la batterie plus longue
- Température de fonctionnement moins élevée
- Durée de charge plus courte
- Réduction des risques
- Optimisation des matières premières

- Autonomie de la batterie plus longue
- Durée de vie de la batterie plus longue
- Température de fonctionnement moins élevée
- Durée de charge plus courte
- Réduction des risques
- Optimisation des matières premières
- Optimisation du prix

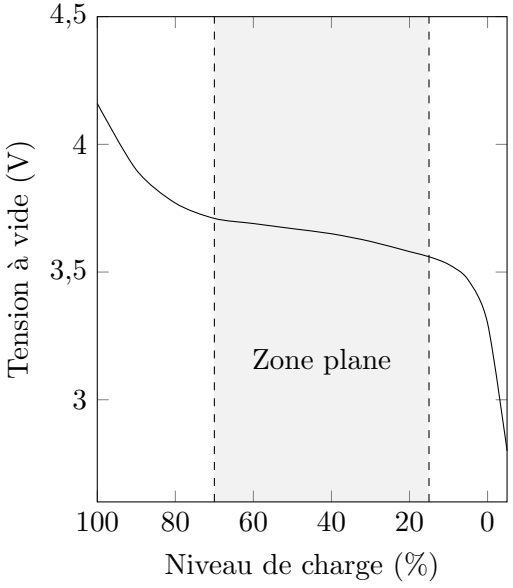
- Comportement non linéaire



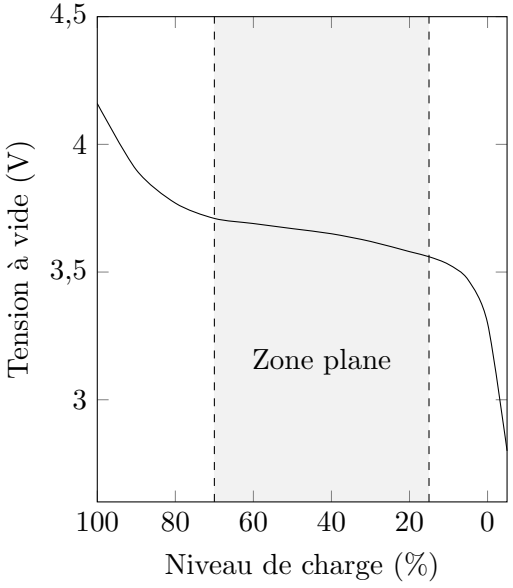
- Comportement non linéaire
- Contraintes de mesure du signal



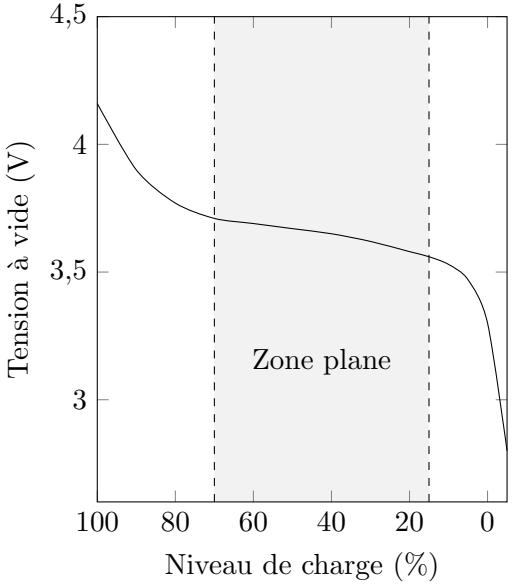
- Comportement non linéaire
- Contraintes de mesure du signal
- Comportement dépendant de :
  - la température de fonctionnement



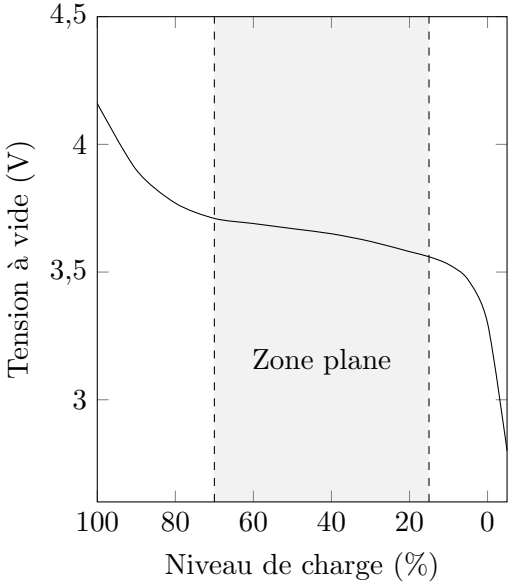
- Comportement non linéaire
- Contraintes de mesure du signal
- Comportement dépendant de :
  - la température de fonctionnement
  - l'âge de la batterie



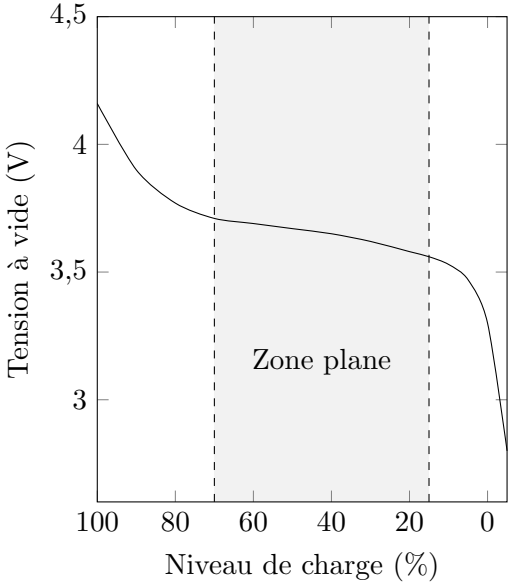
- Comportement non linéaire
- Contraintes de mesure du signal
- Comportement dépendant de :
  - la température de fonctionnement
  - l'âge de la batterie
  - la qualité des ressources utilisées



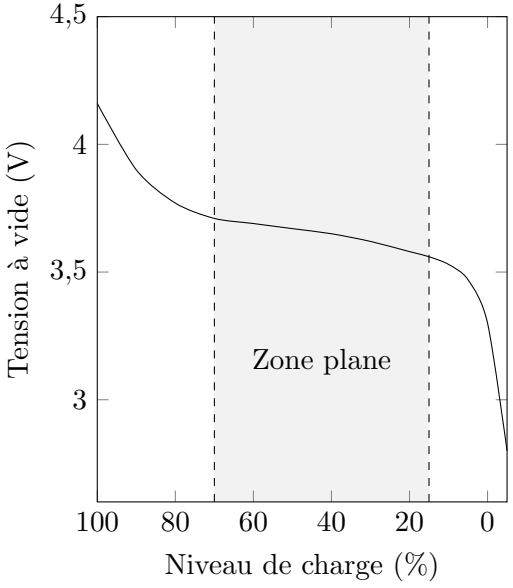
- Comportement non linéaire
- Contraintes de mesure du signal
- Comportement dépendant de :
  - la température de fonctionnement
  - l'âge de la batterie
  - la qualité des ressources utilisées
  - leur utilisation



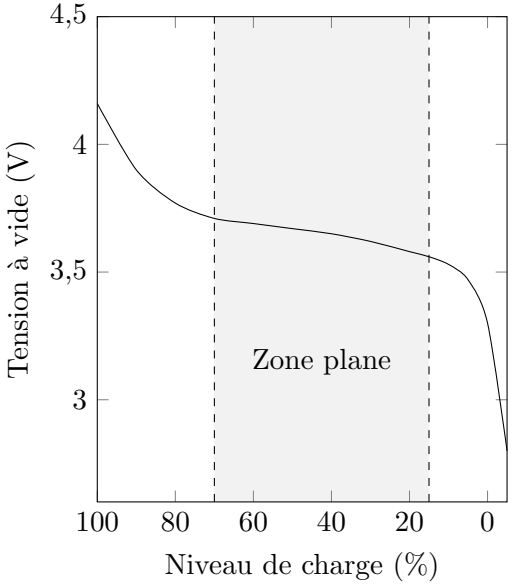
- Comportement non linéaire
- Contraintes de mesure du signal
- Comportement dépendant de :
  - la température de fonctionnement
  - l'âge de la batterie
  - la qualité des ressources utilisées
  - leur utilisation
- Risque de combustion voir d'explosion



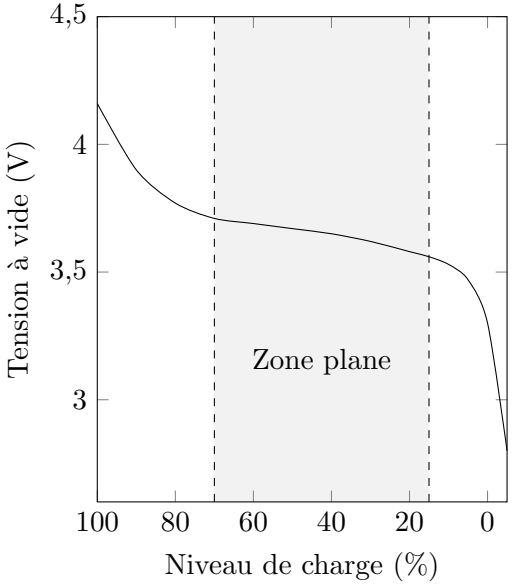
- Comportement non linéaire
- Contraintes de mesure du signal
- Comportement dépendant de :
  - la température de fonctionnement
  - l'âge de la batterie
  - la qualité des ressources utilisées
  - leur utilisation
- Risque de combustion voir d'explosion
- Déséquilibres entre les cellules

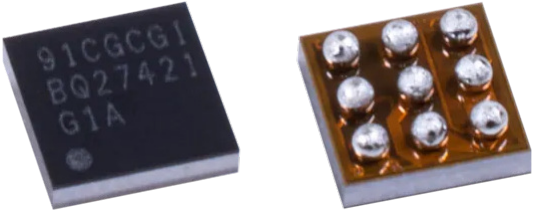


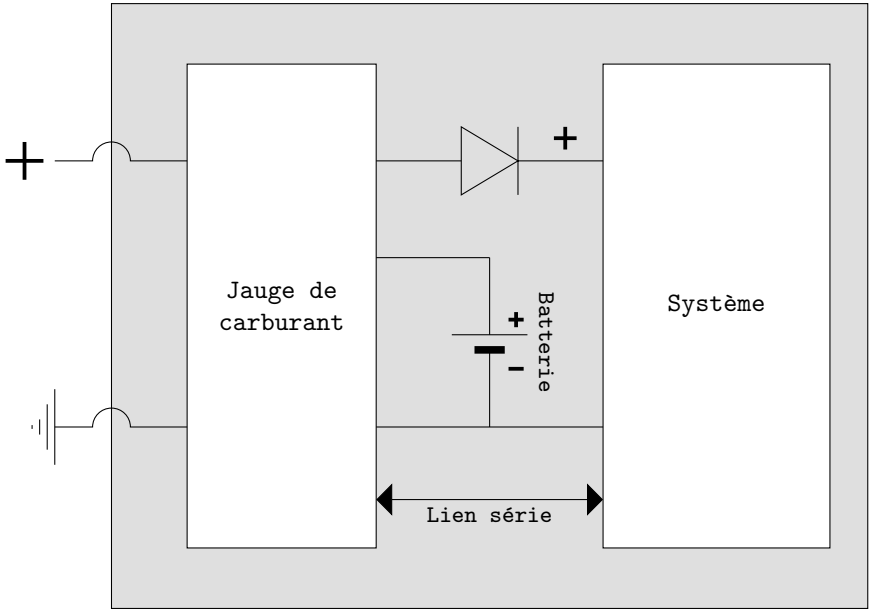
- Comportement non linéaire
- Contraintes de mesure du signal
- Comportement dépendant de :
  - la température de fonctionnement
  - l'âge de la batterie
  - la qualité des ressources utilisées
  - leur utilisation
- Risque de combustion voir d'explosion
- Déséquilibres entre les cellules
- Charge intelligente

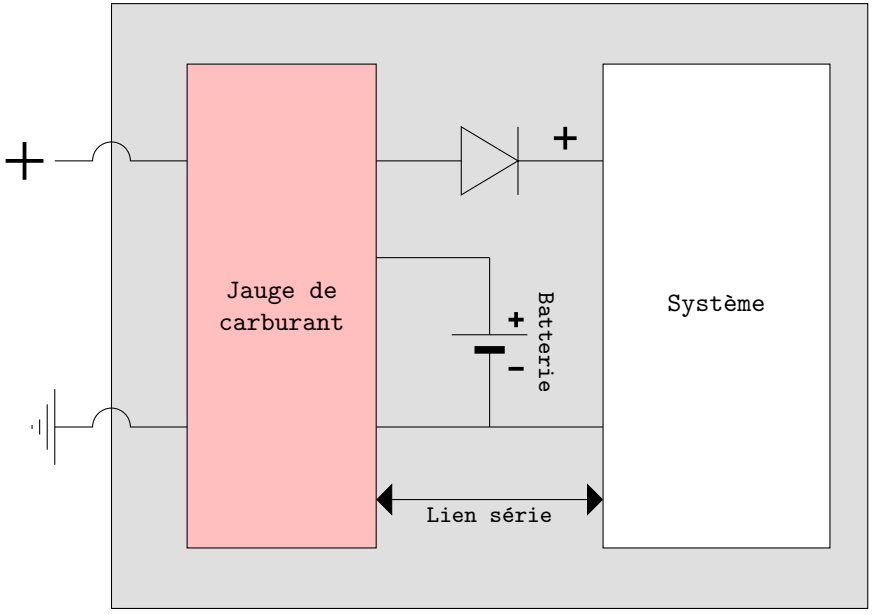


- Comportement non linéaire
- Contraintes de mesure du signal
- Comportement dépendant de :
  - la température de fonctionnement
  - l'âge de la batterie
  - la qualité des ressources utilisées
  - leur utilisation
- Risque de combustion voir d'explosion
- Déséquilibres entre les cellules
- Charge intelligente
- Utilisation de l'énergie irrégulière et imprévisible




91CGCGI
BQ27421
G1A


+
Jauge de carburant
+
Batterie
+
-
Système
Lien série


+
Jauge de carburant
+
Batterie
+
-
Système
Lien série

- Santé de la batterie
- Statut de charge
- Source de charge
- Courant instantané
- Capacité
- Température
- Tension
- Niveau de charge
- Compteur d'énergie

- Santé de la batterie
- Statut de charge
- Source de charge

- Courant instantané
- Capacité
- Température
- Tension
- Niveau de charge
- Compteur d'énergie

`FOREGROUND_SERVICE`

`HIGH_SAMPLING_RATE_SENSORS`

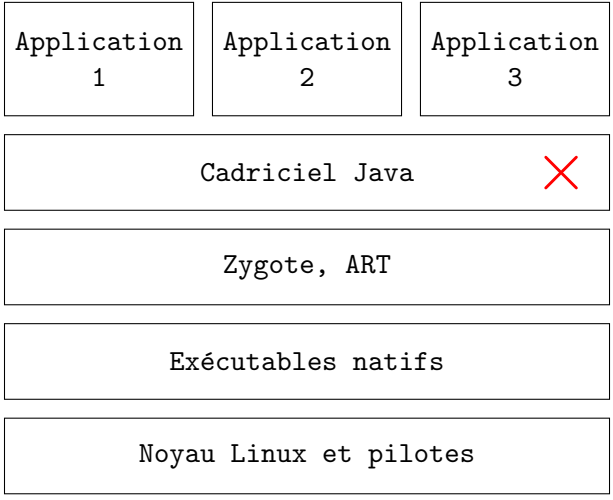
- Santé de la batterie
- Statut de charge
- Source de charge

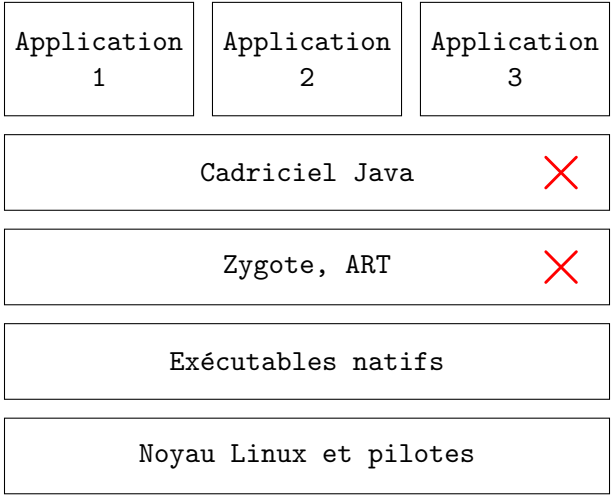
- Courant instantané
- Capacité
- Température
- Tension
- Niveau de charge
- Compteur d'énergie

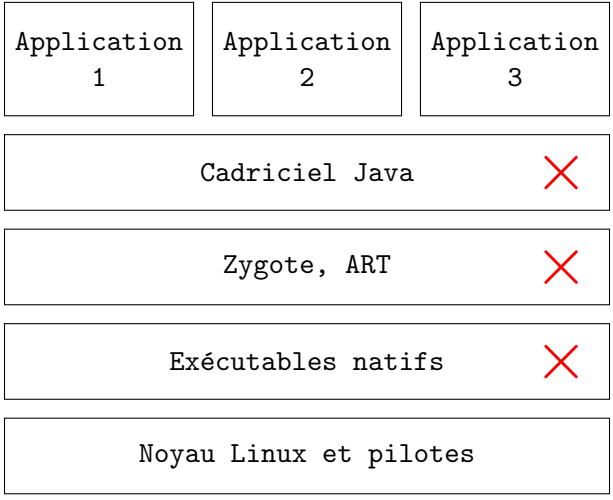
FOREGROUND_SERVICE

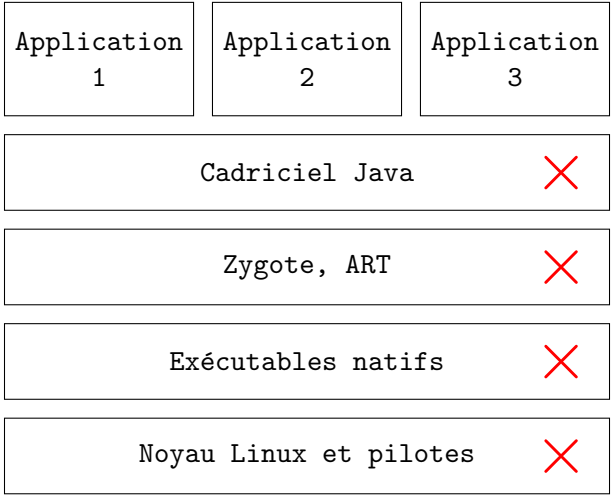
HIGH_SAMPLING_RATE_SENSORS

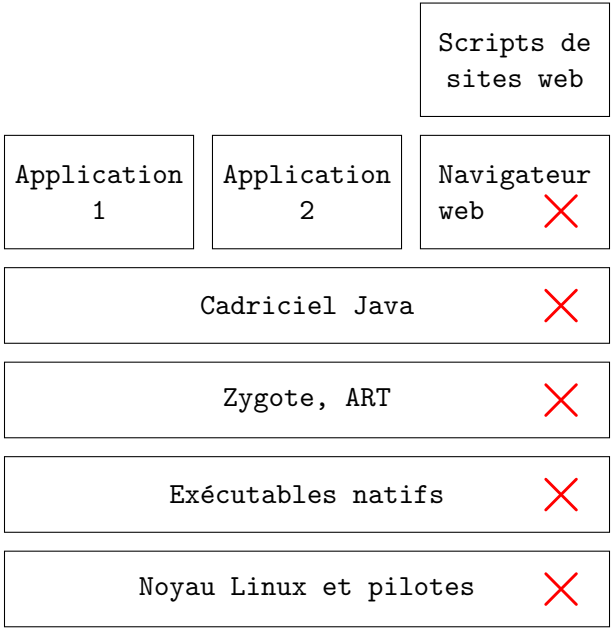
```java
/**
 * Checks if a sensor should be capped according to HIGH_SAMPLING_RATE_SENSORS permission.
 * [...]
 */
private boolean isSensorInCappedSet(int sensorType) {
    return (sensorType == Sensor.TYPE_ACCELEROMETER
            || sensorType == Sensor.TYPE_ACCELEROMETER_UNCALIBRATED
            || sensorType == Sensor.TYPE_GYROSCOPE
            || sensorType == Sensor.TYPE_GYROSCOPE_UNCALIBRATED
            || sensorType == Sensor.TYPE_MAGNETIC_FIELD
            || sensorType == Sensor.TYPE_MAGNETIC_FIELD_UNCALIBRATED);
    }
```

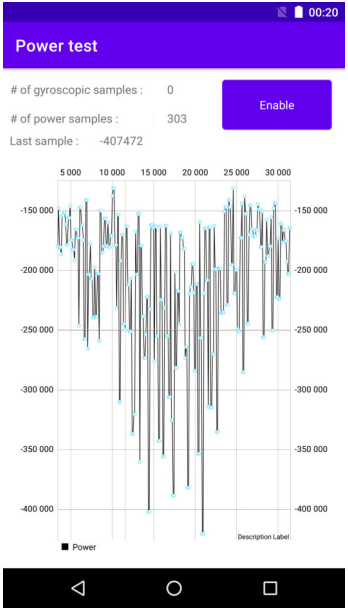

Application 1
Application 2
Application 3
Cadriciel Java
Zygote, ART
Exécutables natifs
Noyau Linux et pilotes

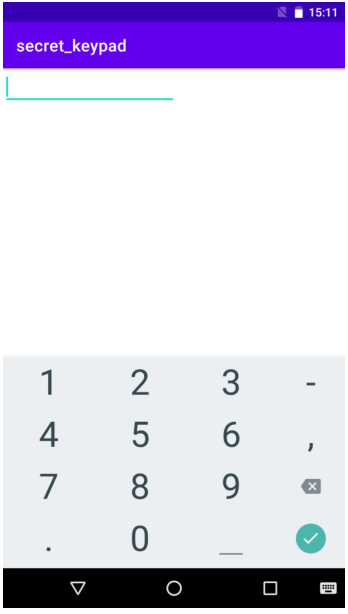

Application 1
Application 2
Application 3
Cadriciel Java
Zygote, ART
Exécutables natifs
Noyau Linux et pilotes

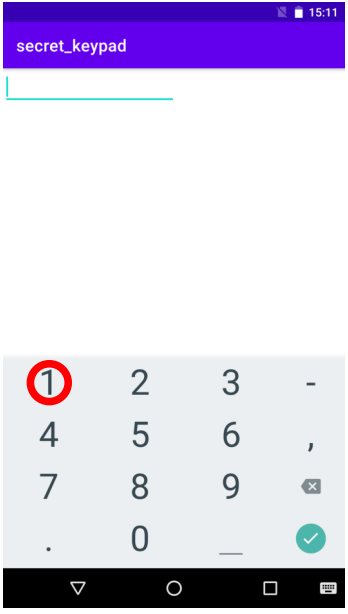

Application 1
Application 2
Application 3
Cadriciel Java
Zygote, ART
Exécutables natifs
Noyau Linux et pilotes

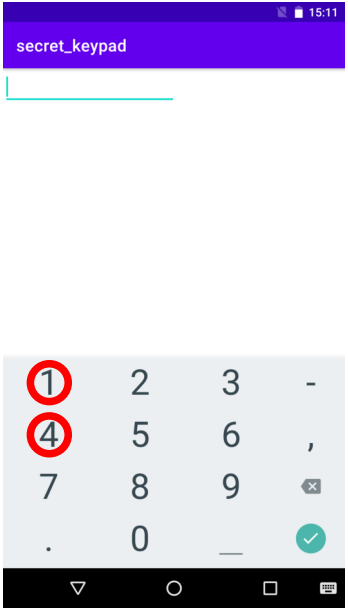

Application 1
Application 2
Application 3
Cadriciel Java
Zygote, ART
Exécutables natifs
Noyau Linux et pilotes

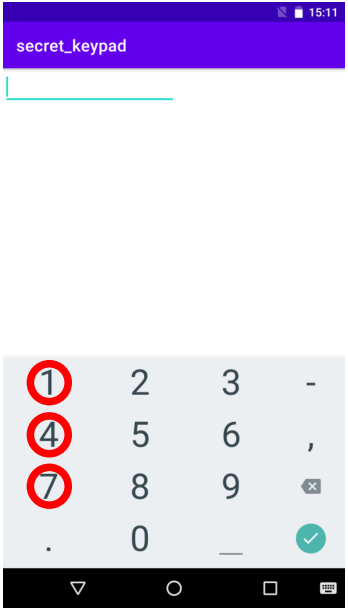

Scripts de sites web
Application 1
Application 2
Navigateur web
Cadriciel Java
Zygote, ART
Exécutables natifs
Noyau Linux et pilotes

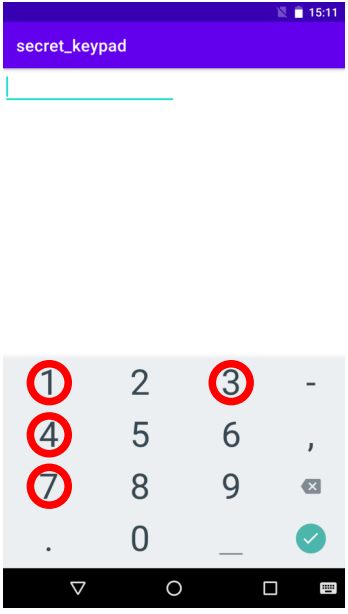

00:20
Power test
# of gyroscopic samples : 0
# of power samples : 303
Last sample : -407472
Enable
5 000
10 000
15 000
20 000
25 000
30 000
-150 000
-200 000
-250 000
-300 000
-350 000
-400 000
Description Label
Power

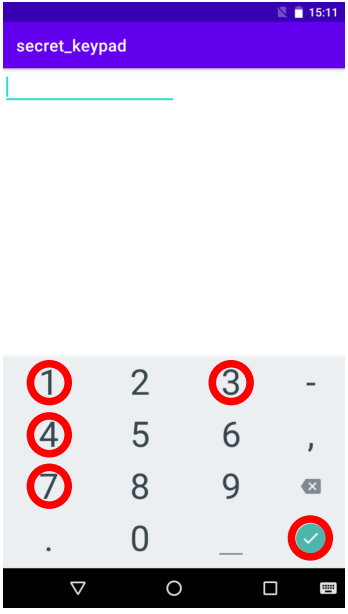

15:11
secret_keypad
1 2 3 -
4 5 6 ,
7 8 9
. 0 _

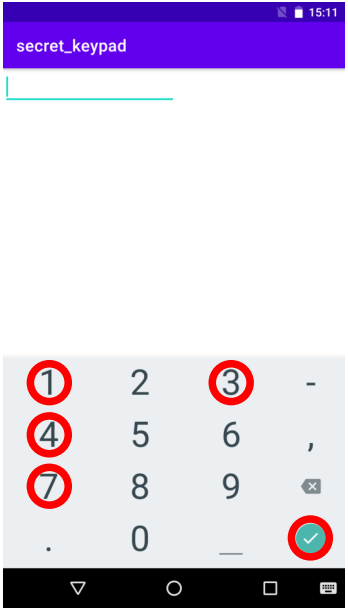

15:11
secret_keypad
1 2 3 -
4 5 6 ,
7 8 9
. 0 _

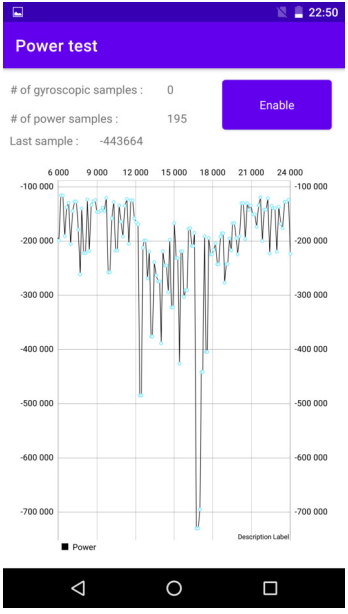

15:11
secret_keypad
1 2 3 -
4 5 6 ,
7 8 9
. 0 _

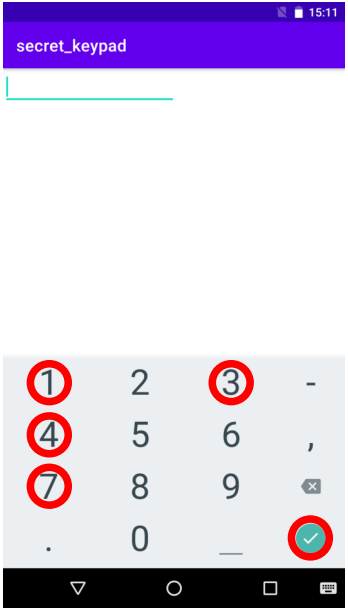

15:11
secret_keypad
1
2
3
-
4
5
6
,
7
8
9
.
0

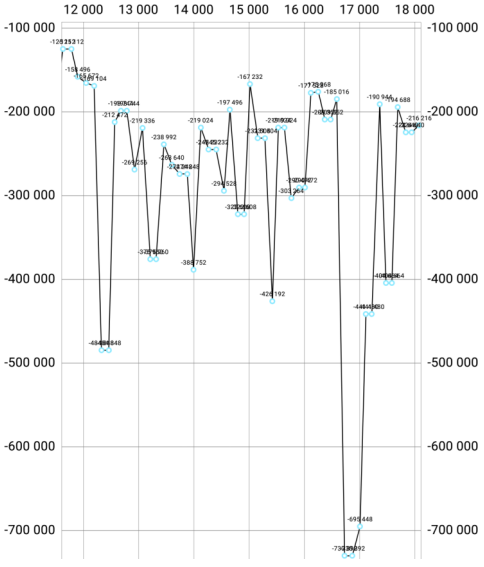

15:11
secret_keypad
1
2
3
-
4
5
6
,
7
8
9
.
0
_

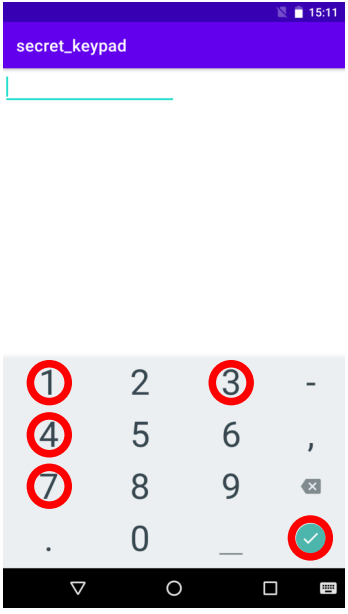

15:11
secret_keypad
1
2
3
-
4
5
6
,
7
8
9
.
0
_

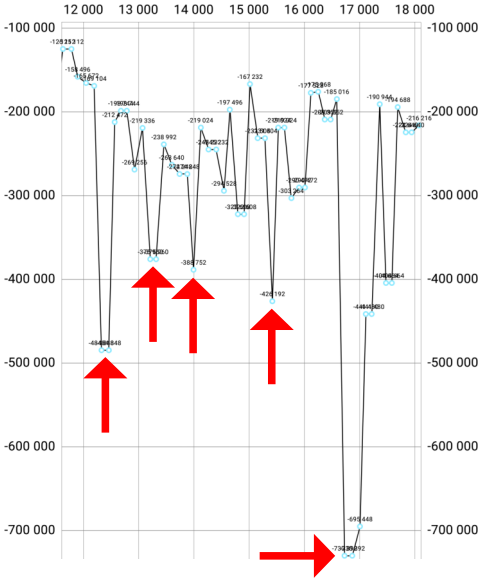

15:11
secret_keypad
1
2
3
-
4
5
6
,
7
8
9
.
0
_

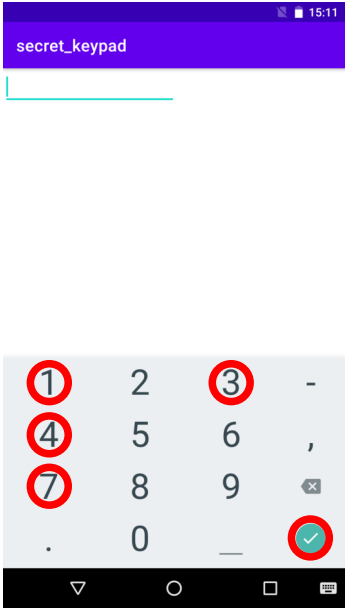

22:50
Power test
# of gyroscopic samples : 0
# of power samples : 195
Last sample : -443664
Enable
6 000
9 000
12 000
15 000
18 000
21 000
24 000
-100 000
-200 000
-300 000
-400 000
-500 000
-600 000
-700 000
Description Label
Power

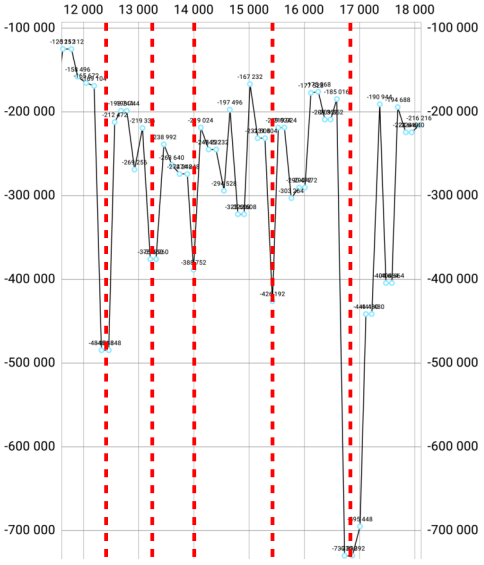

15:11
secret_keypad
1
2
3
-
4
5
6
,
7
8
9
.
0
_

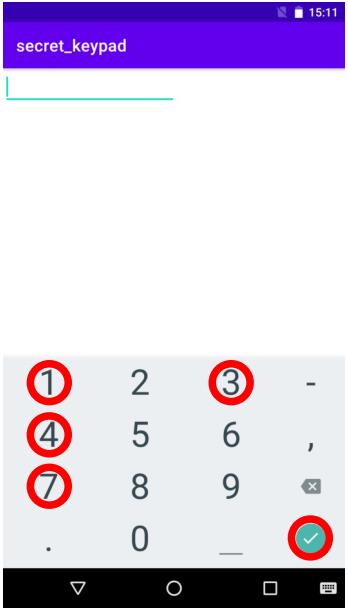

12 000
13 000
14 000
15 000
16 000
17 000
18 000
-100 000
-200 000
-300 000
-400 000
-500 000
-600 000
-700 000

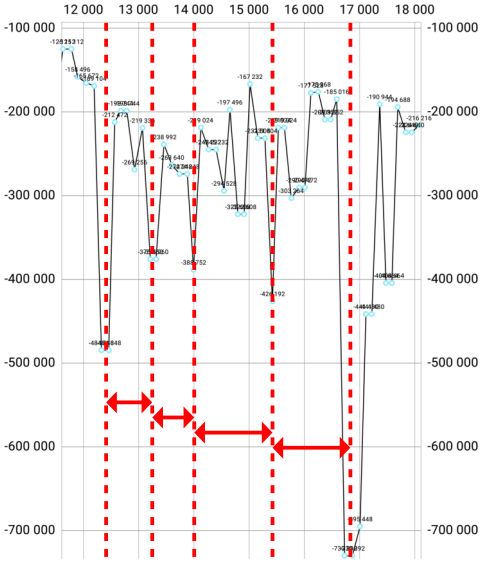

15:11
secret_keypad
1
2
3
-
4
5
6
,
7
8
9
.
0

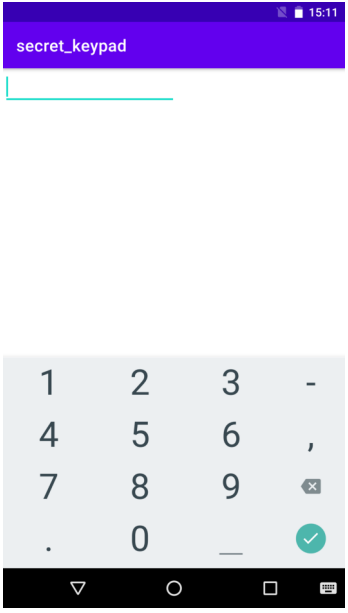

12 000
13 000
14 000
15 000
16 000
17 000
18 000
-100 000
-200 000
-300 000
-400 000
-500 000
-600 000
-700 000

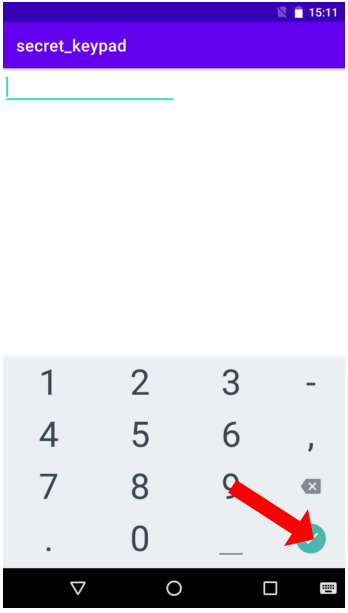

15:11
secret_keypad
1
2
3
-
4
5
6
,
7
8
9
.
0

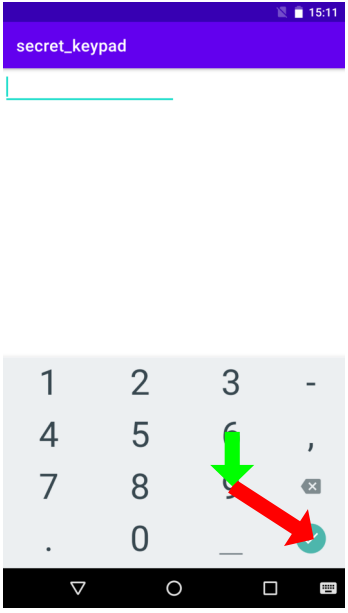

12 000
13 000
14 000
15 000
16 000
17 000
18 000
-100 000
-200 000
-300 000
-400 000
-500 000
-600 000
-700 000

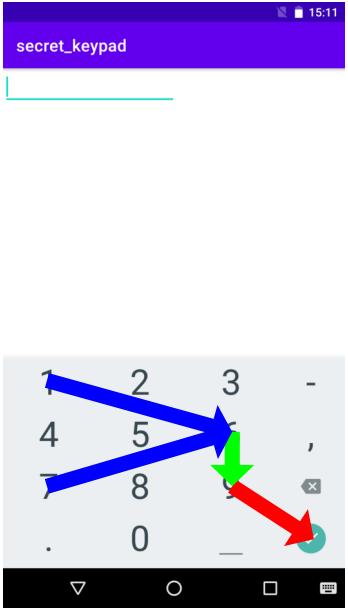

15:11
secret_keypad
1
2
3
-
4
5
6
,
7
8
9
.
0

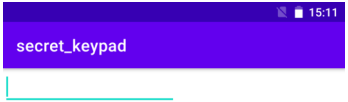

12 000
13 000
14 000
15 000
16 000
17 000
18 000
-100 000
-200 000
-300 000
-400 000
-500 000
-600 000
-700 000

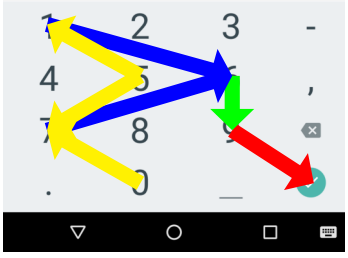

15:11
secret_keypad
1 2 3 -
4 5 6 ,
7 8 9
. 0 _


15:11
secret_keypad
1 2 3 -
4 5 6 ,
7 8 9
. 0 _

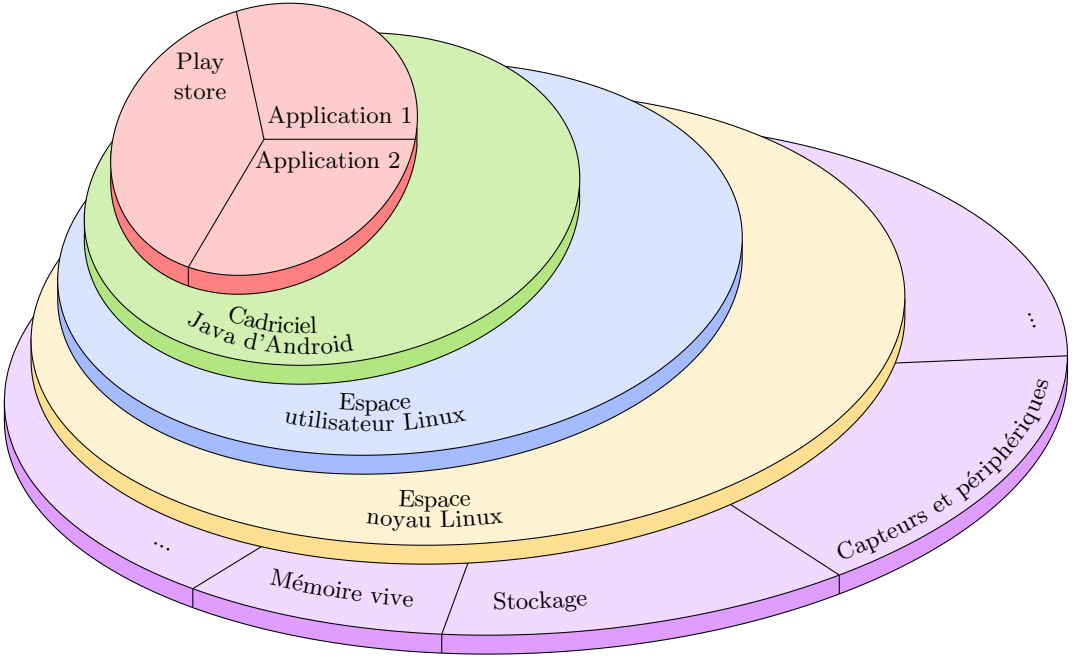

15:11
secret_keypad
1 2 3 -
4 5 6 ,
7 8 9
. 0 _

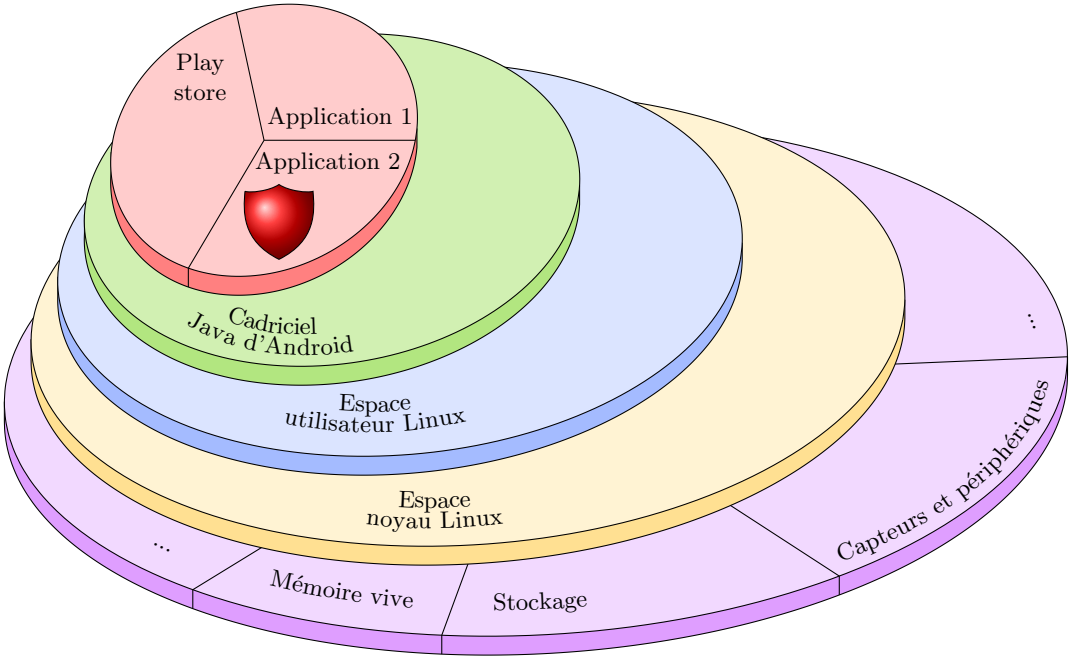

15:11
secret_keypad
1
2
3
-
4
5
,
8
.
0

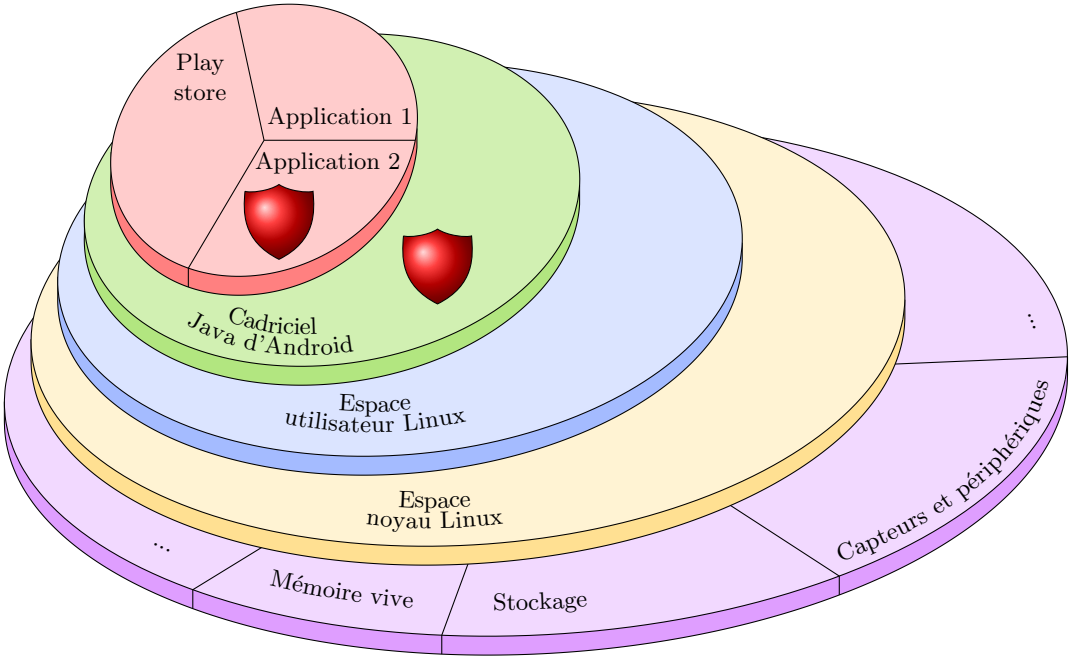

15:11
secret_keypad


2
3
-
4
,
8
.
0

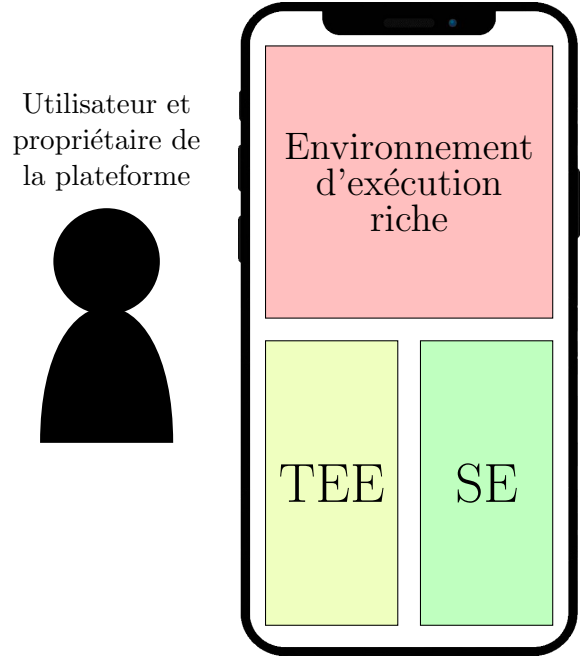
```
1 (arbre '(3.37 4.01 1 1) (cons '(10) '()) 0)
2 => ((((((10 3 7 4 7) (10 3 7 4 1))))))
```


Play
store
Application 1
Application 2
Cadriciel
Java d'Android
Espace
utilisateur Linux
Espace
noyau Linux
...
Capteurs et périphériques
...
Mémoire vive
Stockage

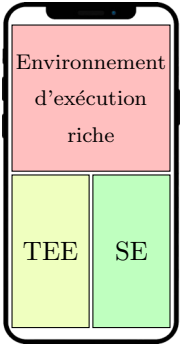

Play
store
Application 1
Application 2
Cadriciel
Java d'Android
Espace
utilisateur Linux
Espace
noyau Linux
...
Mémoire vive
Stockage
Capteurs et périphériques
...

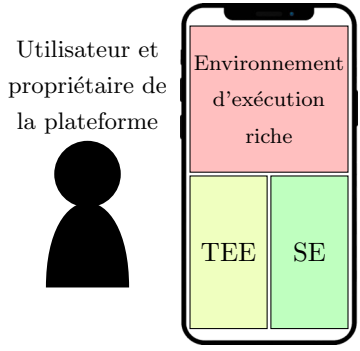

Play
store
Application 1
Application 2
Cadriciel
Java d'Android
Espace
utilisateur Linux
Espace
noyau Linux
...
Capteurs et périphériques
...
Mémoire vive
Stockage

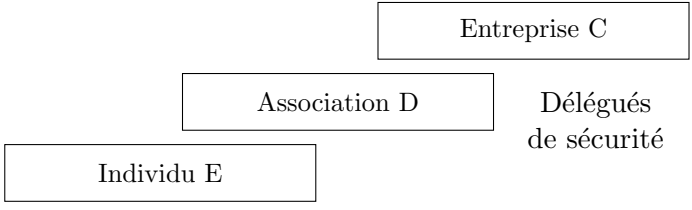
Propositions

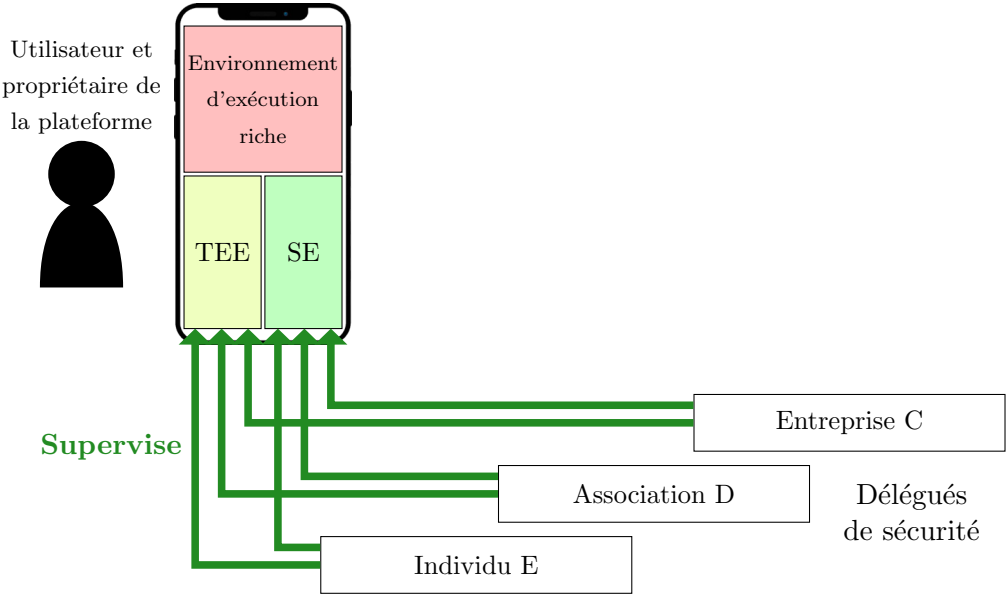

Utilisateur et propriétaire de la plateforme
Environnement d'exécution riche
TEE
SE

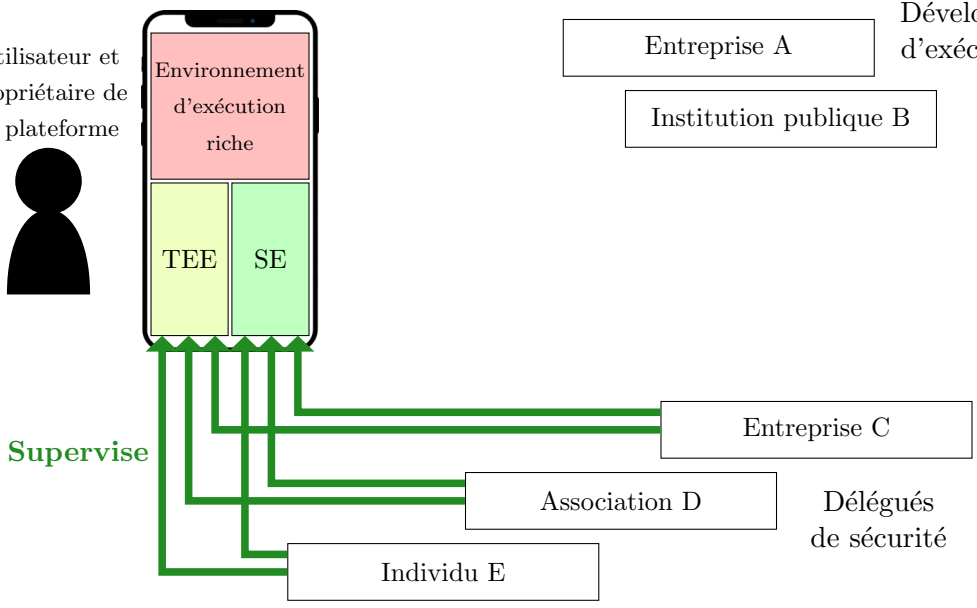
Utilisateur et propriétaire de la plateforme

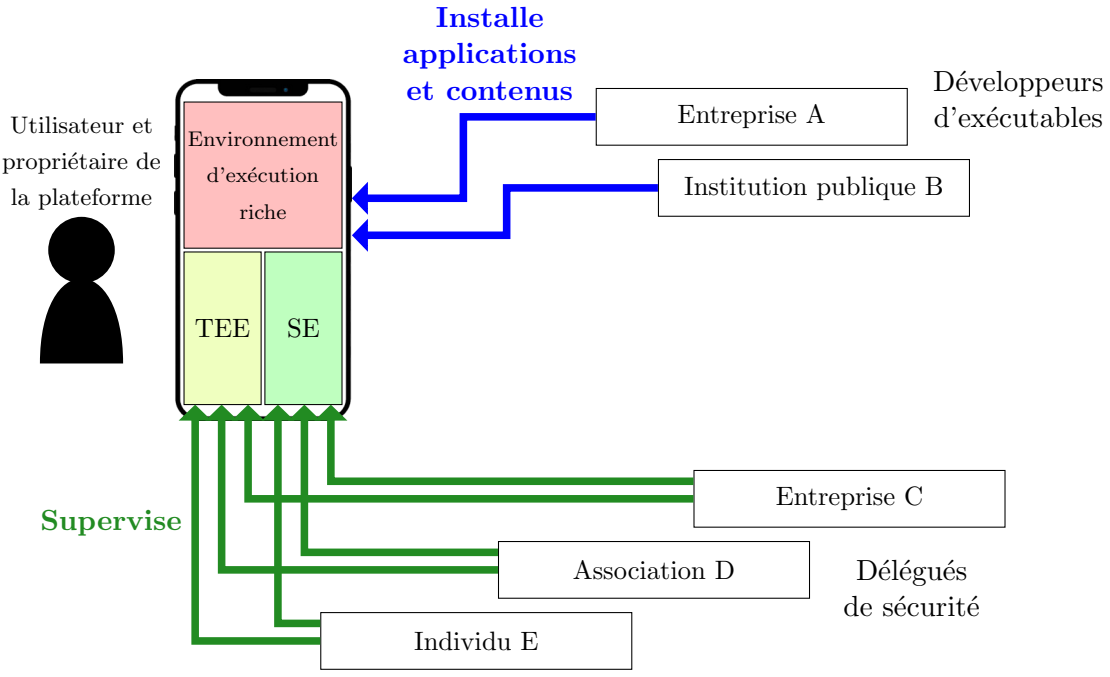


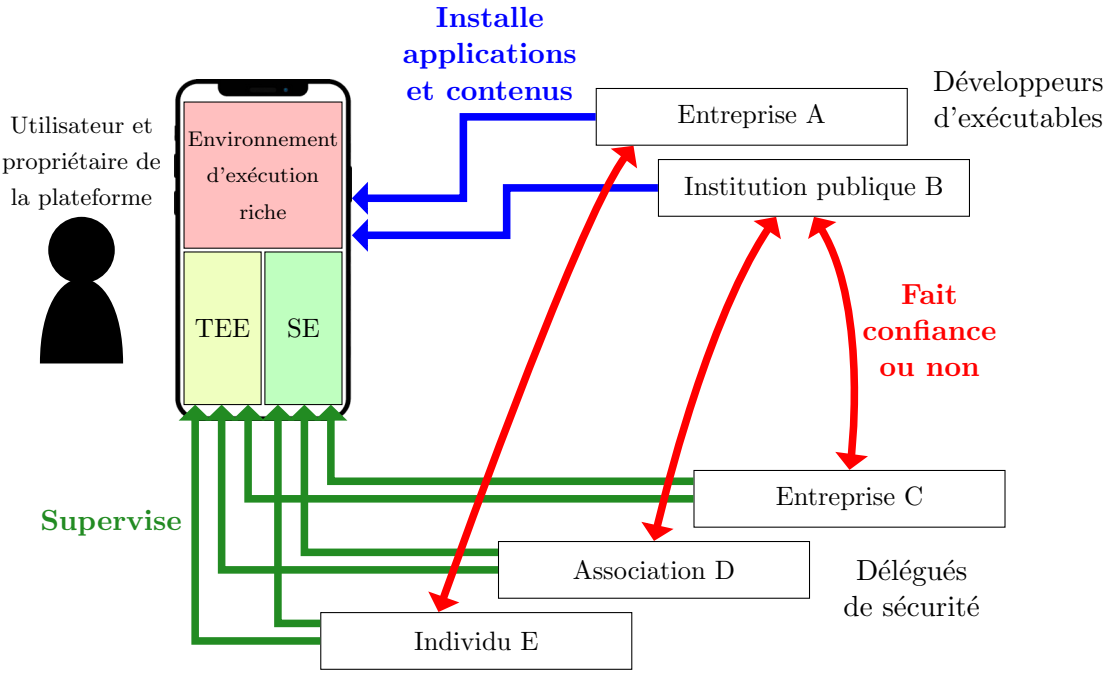

Utilisateur et propriétaire de la plateforme
Environnement d'exécution riche
TEE
SE


Entreprise C
Association D
Délégués de sécurité
Individu E


Utilisateur et propriétaire de la plateforme
Environnement d'exécution riche
TEE
SE
Supervise
Entreprise C
Association D
Individu E
Délégués de sécurité


Utilisateur et propriétaire de la plateforme
Environnement d'exécution riche
TEE
SE
Développeurs d'exécutables
Entreprise A
Institution publique B
Supervise
Entreprise C
Association D
Délégués de sécurité
Individu E


Installe applications et contenus
Développeurs d'exécutables
Entreprise A
Institution publique B
Utilisateur et propriétaire de la plateforme
Environnement d'exécution riche
TEE
SE
Supervise
Entreprise C
Association D
Délégués de sécurité
Individu E


Installe
applications
et contenus
Développeurs
d'exécutables
Utilisateur et
propriétaire de
la plateforme
Environnement
d'exécution
riche
TEE
SE
Entreprise A
Institution publique B
Fait
confiance
ou non
Supervise
Entreprise C
Association D
Délégués
de sécurité
Individu E

Constructeurs de composants sécurisés

Délégués de sécurité

Entreprise C

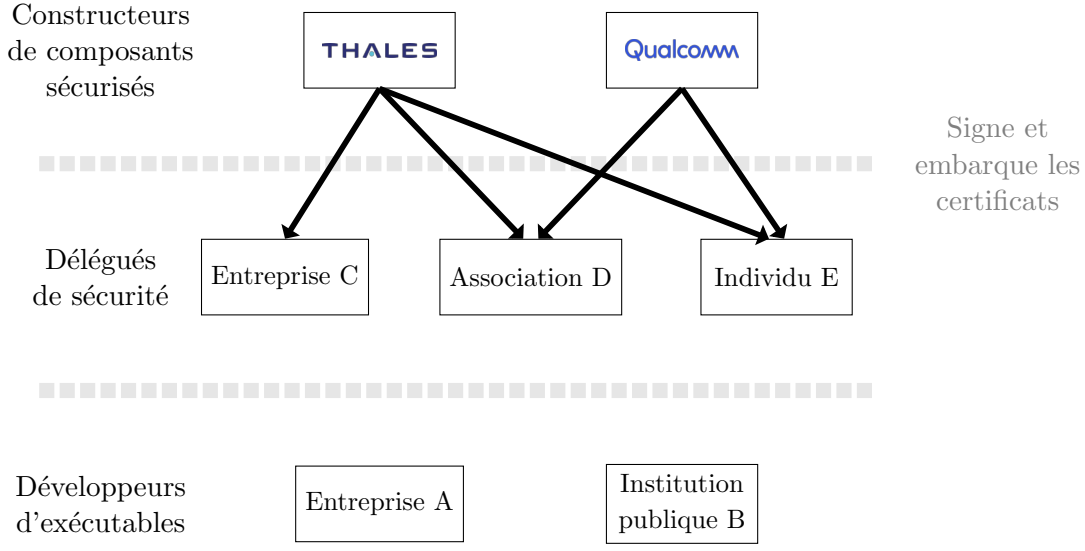
Association D

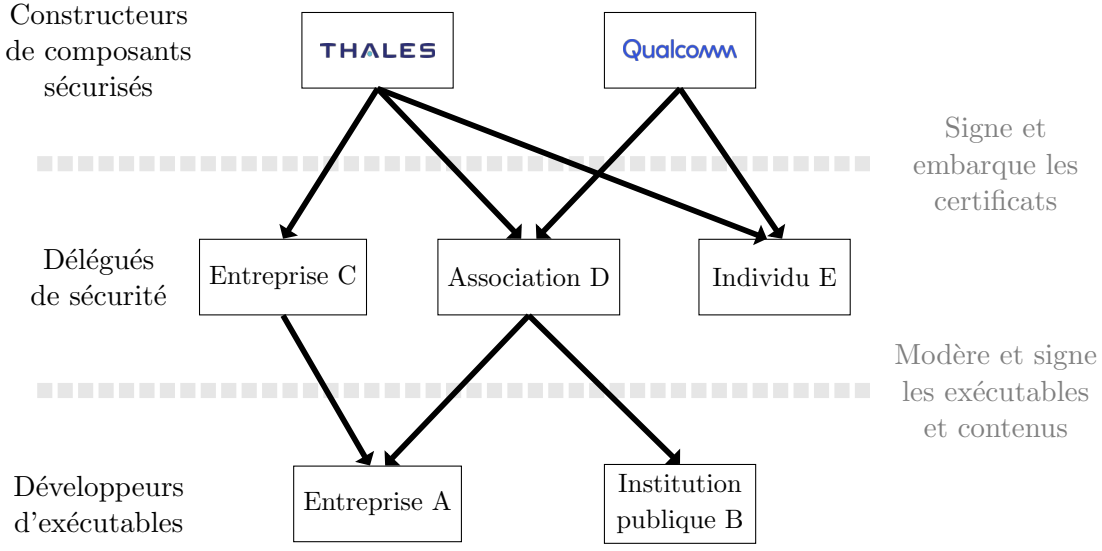
Individu E

Développeurs d'exécutables

Entreprise A

Institution publique B


Constructeurs de composants sécurisés
THALES
Qualcomm
Signe et embarque les certificats
Délégués de sécurité
Entreprise C
Association D
Individu E
Développeurs d'exécutables
Entreprise A
Institution publique B


Constructeurs de composants sécurisés
THALES
Qualcomm
Signe et embarque les certificats
Délégués de sécurité
Entreprise C
Association D
Individu E
Modère et signe les exécutables et contenus
Développeurs d'exécutables
Entreprise A
Institution publique B

Constructeurs
de cor
séc

ne et
rque les
ifications

Dé
de s

e et signe
cutables
ntenus

Déve
d'exécutables

publique B

GSMA™

Conclusion

- Présentation et analyse des **enjeux** et **intérêts** liés à la sécurité des applications sur les systèmes informatiques sur étagère

- Présentation et analyse des **enjeux** et **intérêts** liés à la sécurité des applications sur les systèmes informatiques sur étagère
- Investigation autour des **risques** présents en pratique

- Présentation et analyse des **enjeux** et **intérêts** liés à la sécurité des applications sur les systèmes informatiques sur étagère
- Investigation autour des **risques** présents en pratique
- Propositions de **protections**

- Poursuite des travaux sur McEliece

- Poursuite des travaux sur McEliece
- Investigation supplémentaire dans Android

- Poursuite des travaux sur McEliece
- Investigation supplémentaire dans Android
- Extension de la confiance vers les environnements riches

Publications académiques

- *Journée thématique sur les Attaques par Injection de Fautes* (JAIF) 2022 : *L'attaque en faute : la bête noire des boîtes blanches.*
- *Security of Software/Hardware Interfaces* (SILM) 2023 au sein d'*European Symposium on Security and Privacy* (EuroS&P) : *Faulting original McEliece's implementations is possible — How to mitigate this risk ?*
- *Symposium sur la Sécurité des Technologies de l'Information et des Communications* (SSTIC) 2023 : *Batterie à bord, quand les jauges de carburant dépassent les limites.*
- *International Workshop on Security* (IWSEC) 2023 : *Power analysis pushed too far — Breaking Android-based isolation with fuel gauges.* Publication associée dans *Lecture Notes in Computer Science* (LNCS), volume 14128.

Brevets

- Brevet numéro WO2024083849, date de priorité au 17 octobre 2022 : *encodage en boîte blanche*
- Brevet numéro WO2024083855, date de priorité au 17 octobre 2022 : *clés cryptographiques en boîte blanche*
- Brevet numéro WO2024121142, date de priorité au 6 décembre 2022 : *procédé de protection d'un terminal contre une attaque par canal auxiliaire*

[Ava+10] R. M. Avanzi et al. “Side-Channel Attacks on the McEliece and Niederreiter Public-Key Cryptosystems”. (2010). https://eprint.iacr.org/2010/479.

[BGE05] Olivier Billet, Henri Gilbert et Charaf Ech-Chatbi. “Cryptanalysis of a White Box AES Implementation”. Selected Areas in Cryptography. Lecture Notes in Computer Science. 2005.

[Boc+18] Estuardo Alpirez Bock et al. “On the Ineffectiveness of Internal Encodings - Revisiting the DCA Attack on White-Box Cryptography”. (2018). https://eprint.iacr.org/2018/301.

[Bos+15] Joppe W. Bos et al. “Differential Computation Analysis : Hiding Your White-Box Designs Is Not Enough”. (2015). https://eprint.iacr.org/2015/753.

[Che+14] Cong Chen et al. “Differential Power Analysis of a McEliece Cryptosystem”. (2014). https://eprint.iacr.org/2014/534.

[Cho+03a] Stanley Chow et al. “A White-Box DES Implementation for DRM Applications”. Digital Rights Management. 2003. http://link.springer.com/10.1007/978-3-540-44993-5_1.

[Cho+03b] Stanley Chow et al. “White-Box Cryptography and an AES Implementation”. Selected Areas in Cryptography. 2003. http://link.springer.com/10.1007/3-540-36492-7_17.

[CMP14] Alain Couvreur, Irene Márquez-Corbella et Ruud Pellikaan. “A Polynomial Time Attack against Algebraic Geometry Code Based Public Key Cryptosystems”. 2014 IEEE International Symposium on Information Theory. 2014. https://ieeexplore.ieee.org/abstract/document/6875072.

[COT17] Alain Couvreur, Ayoub Otmani et Jean-Pierre Tillich. “Polynomial Time Attack on Wild McEliece Over Quadratic Extensions”. IEEE Transactions on Information Theory (2017). https://ieeexplore.ieee.org/abstract/document/7496988.

[ECJ15] Eloi Sanfelix, Cristofaro Mune et Job de Haas. “Practical Attacks against Obfuscated Ciphers”. (2015).

[Fau+10] Jean-Charles Faugère et al. “Algebraic Cryptanalysis of McEliece Variants with Compact Keys”. Advances in Cryptology – EUROCRYPT 2010. Lecture Notes in Computer Science. 2010.

[FM08] Cédric Faure et Lorenz Minder. “Cryptanalysis of the McEliece Cryptosystem over Hyperelliptic Codes”. Eleventh International Workshop on Algebraic and Combinatorial Coding Theory (2008).

[HMP10] Stefan Heyse, Amir Moradi et Christof Paar. “Practical Power Analysis Attacks on Software Implementations of McEliece”. Post-Quantum Cryptography. Lecture Notes in Computer Science. 2010.

[McE78] R.J. McEliece. “A Public-Key Cryptosystem Based On Algbraic Coding Theory”. (1978).

[Mol+11] H. Gregor Molter et al. “A Simple Power Analysis Attack on a McEliece Cryptoprocessor”. Journal of Cryptographic Engineering (2011). https://doi.org/10.1007/s13389-011-0001-3.

[MS07] Lorenz Minder et Amin Shokrollahi. “Cryptanalysis of the Sidelnikov Cryptosystem”. Advances in Cryptology - EUROCRYPT 2007. Lecture Notes in Computer Science. 2007.

[OTD10] Ayoub Otmani, Jean-Pierre Tillich et Léonard Dallot. “Cryptanalysis of Two McEliece Cryptosystems Based on Quasi-Cyclic Codes”. Mathematics in Computer Science (2010). https://doi.org/10.1007/s11786-009-0015-8.

[Sho+10] Abdulhadi Shoufan et al. “A Timing Attack against Patterson Algorithm in the McEliece PKC”. Information, Security and Cryptology – ICISC 2009. Lecture Notes in Computer Science. 2010.

[SS92] V. M. Sidelnikov et S. O. Shestakov. “On Insecurity of Cryptosystems Based on Generalized Reed-Solomon Codes”. (1992). https://www.degruyter.com/document/doi/10.1515/dma.1992.2.4.439/html.

[Str+08] Falko Strenzke et al. “Side Channels in the McEliece PKC”. Post-Quantum Cryptography. Lecture Notes in Computer Science. 2008.

[Str10] Falko Strenzke. “A Timing Attack against the Secret Permutation in the McEliece PKC”. Post-Quantum Cryptography. Lecture Notes in Computer Science. 2010.

[Str11a] Falko Strenzke. “Message-Aimed Side Channel and Fault Attacks against Public Key Cryptosystems with Homomorphic Properties”. Journal of Cryptographic Engineering (2011). https://doi.org/10.1007/s13389-011-0020-0.

[Str11b] Falko Strenzke. “Timing Attacks against the Syndrome Inversion in Code-based Cryptosystems”. (2011). https://eprint.iacr.org/2011/683.

[VG14] Ingo Von Maurich et Tim Güneysu. “Towards Side-Channel Resistant Implementations of QC-MDPC McEliece Encryption on Constrained Devices”. Post-Quantum Cryptography. Cham, 2014. http://link.springer.com/10.1007/978-3-319-11659-4_16.