

THÈSE DE DOCTORAT
DE L'UNIVERSITÉ PSL

Préparée à l'École Normale Supérieure de Paris

Soutenue par

Vincent Giraud

Le 26 septembre 2024

École doctorale n°386

Sciences Mathématiques de Paris Centre

Spécialité

Informatique

**Sécurité des applications sur
systèmes non maîtrisés.**

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

Composition du jury :

Pascal Lafourcade
Professeur, Université Clermont Auvergne

*Rapporteur et
président du jury*

Clémentine Maurice
Chargée de recherche HDR, CNRS, Lille

Rapporteuse

Aurélien Francillon
Professeur, EURECOM Sophia Antipolis

Examineur

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

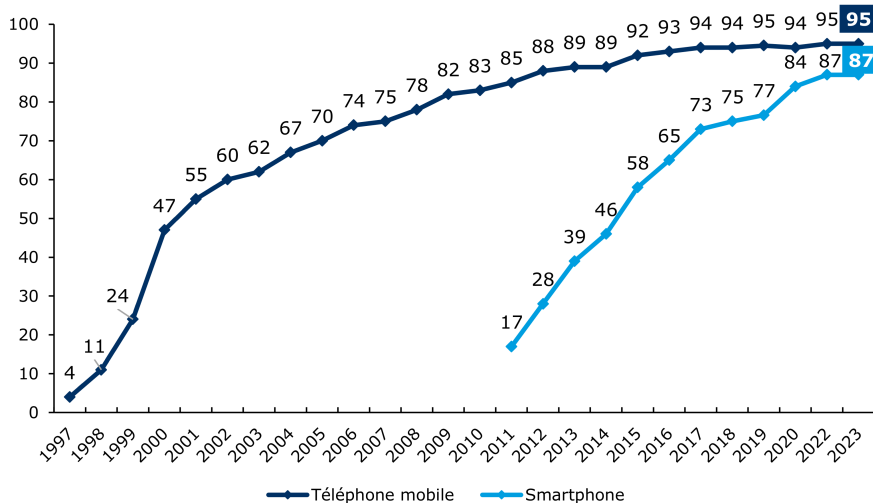
Tania Richmond
Maîtresse de conférences, Université de la Nouvelle-Calédonie

Invitée

Contexte

Taux d'équipement en téléphone mobile et smartphone

- Champ : ensemble de la population de 12 ans et plus, en % -



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

The logo for Apple Pay, featuring a black silhouette of an apple with a bite taken out of it, followed by the word "Pay" in a bold, black, sans-serif font.The logo for Google Pay, featuring the multi-colored "G" logo of Google, followed by the word "Pay" in a grey, sans-serif font.The logo for Samsung Pay, featuring the word "SAMSUNG" in a bold, black, sans-serif font, with the word "Pay" below it in a larger, bold, black, sans-serif font.

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.

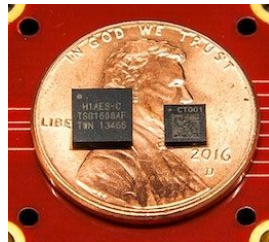
Un système embarqué est un système informatique logiciel et matériel enfoui dans un objet afin de contrôler son activité et sa sécurité, d'offrir des services à ses utilisateurs et de communiquer avec d'autres objets.

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

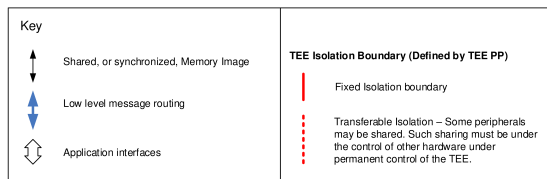
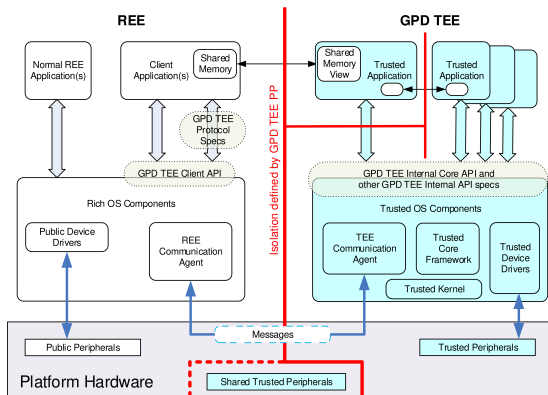
*Un objet communicant permet à l'utilisateur d'accéder à des services via cet objet grâce à un échange d'informations avec le monde qui l'entoure.
Les dispositifs numériques qui permettent d'offrir ces services sont appelés systèmes embarqués.*

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

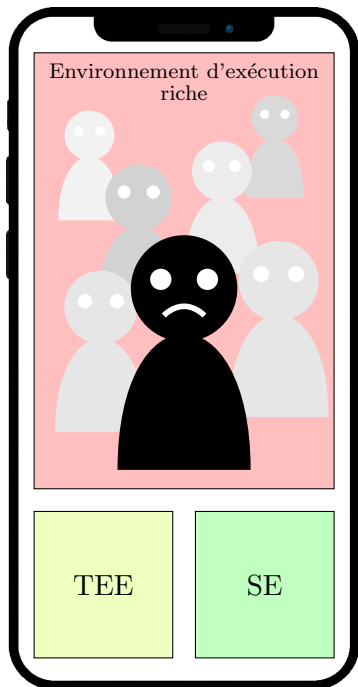
Secure Elements (SE)

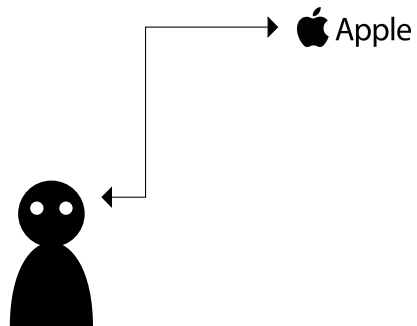
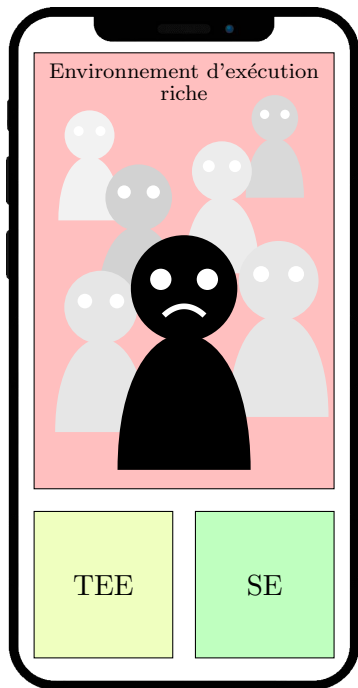


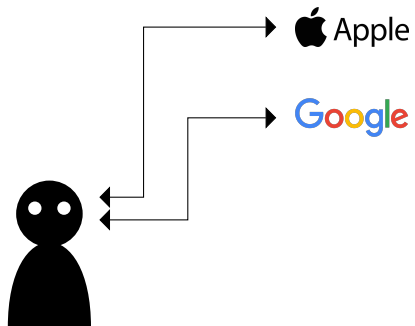
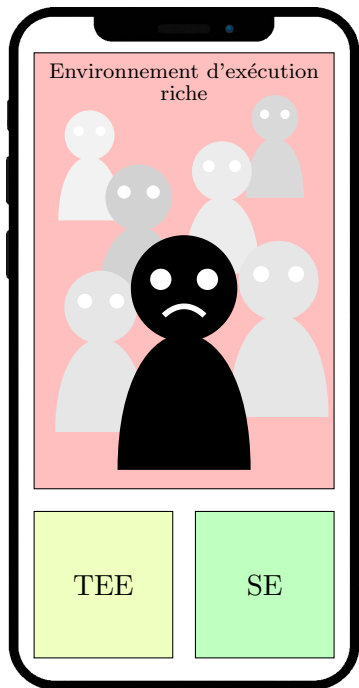
Trusted Execution Environments (TEE)

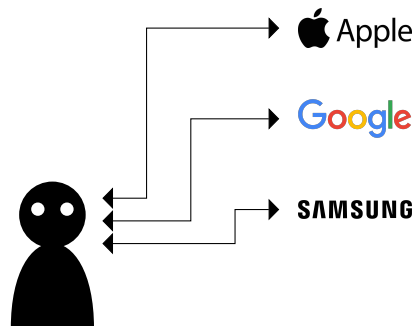
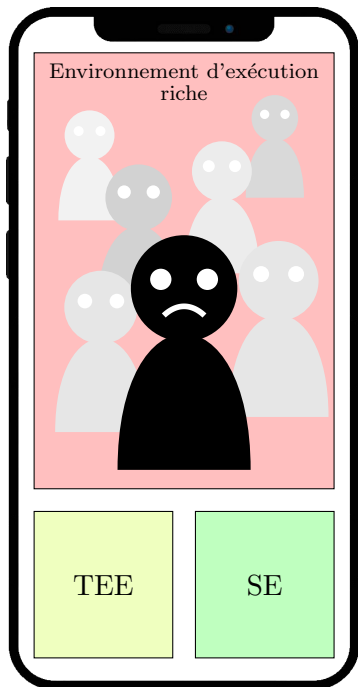


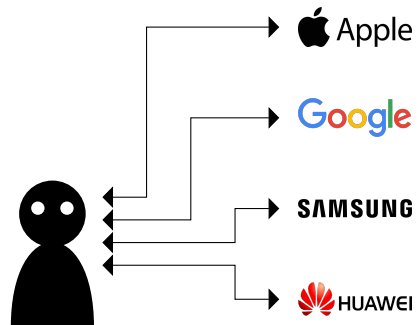
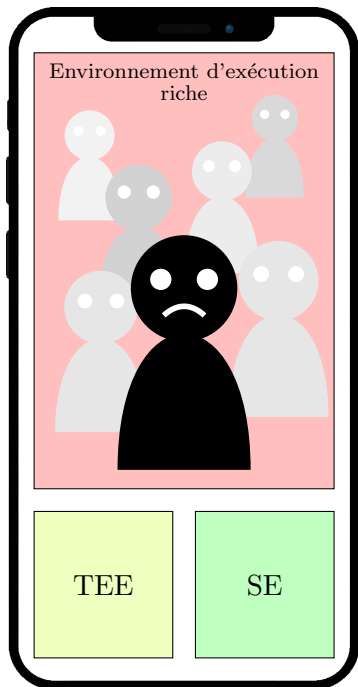
GlobalPlatform, Inc. *TEE Protection Profile*, 2020.

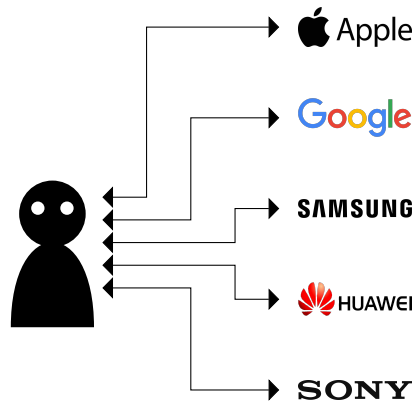
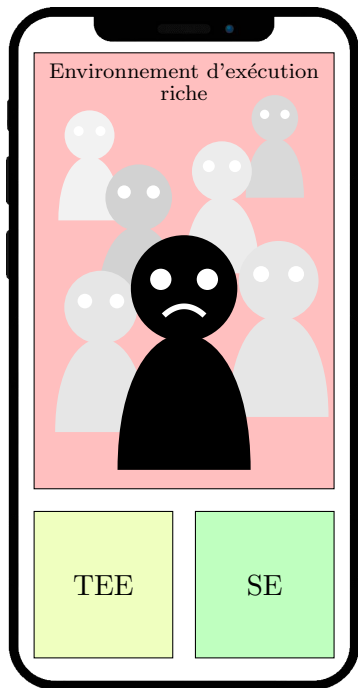


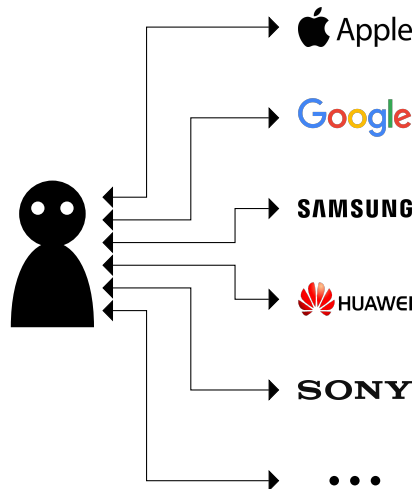
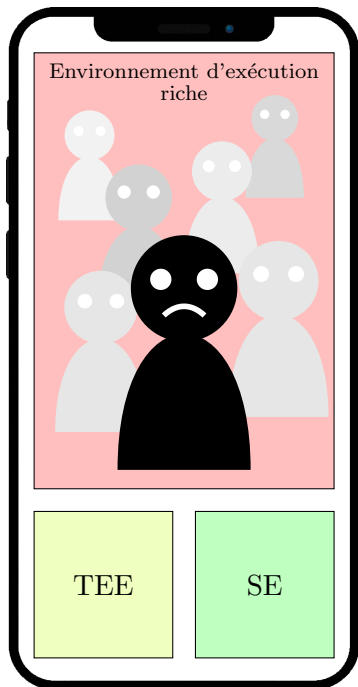








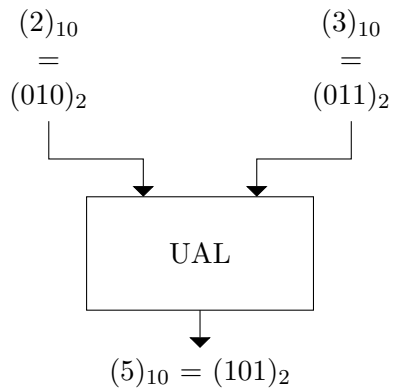




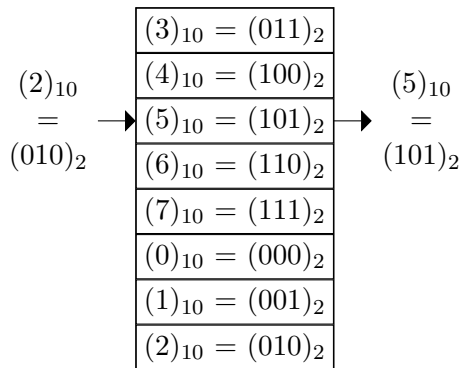
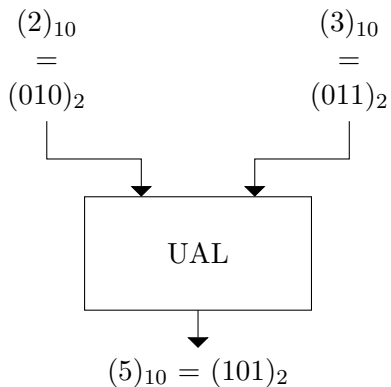
État de l'art

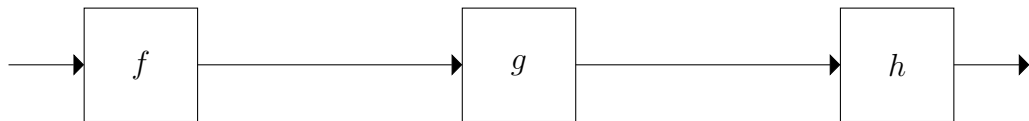
Cryptographie en boîte blanche

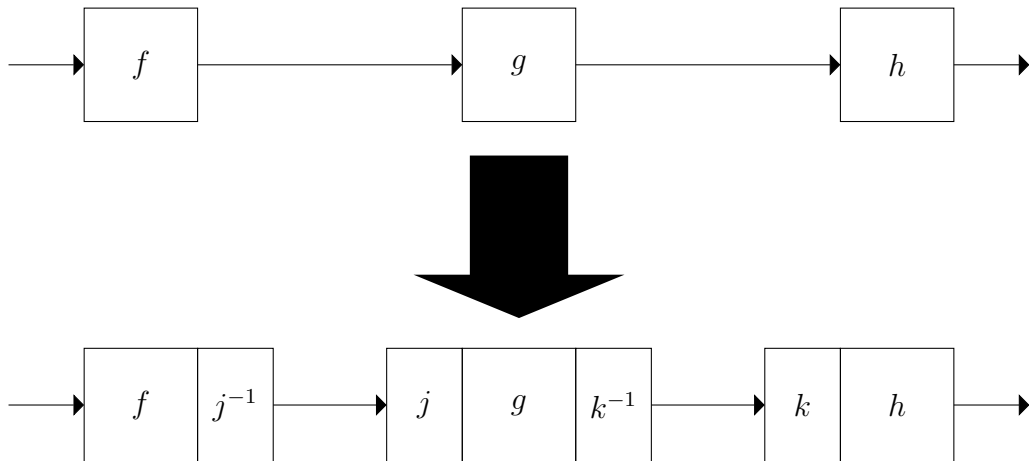
[Cho+03b; Cho+03a]



[Cho+03b; Cho+03a]







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



BGE

[BGE05]

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

A yellow starburst shape with a red outline, containing the text 'BGE' and '[BGE05]'.

BGE

[BGE05]

La sécur

le sav

en bo

et que nécessit

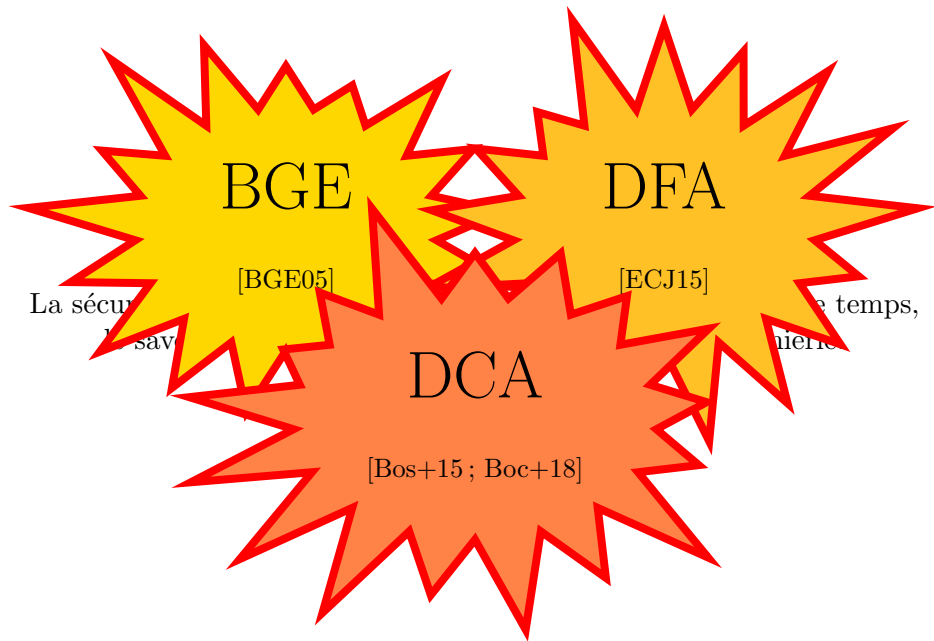
A yellow starburst shape with a red outline, containing the text 'DFA' and '[ECJ15]'.

DFA

[ECJ15]

e temps,

niens





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.	<i>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.</i>

État de l'art

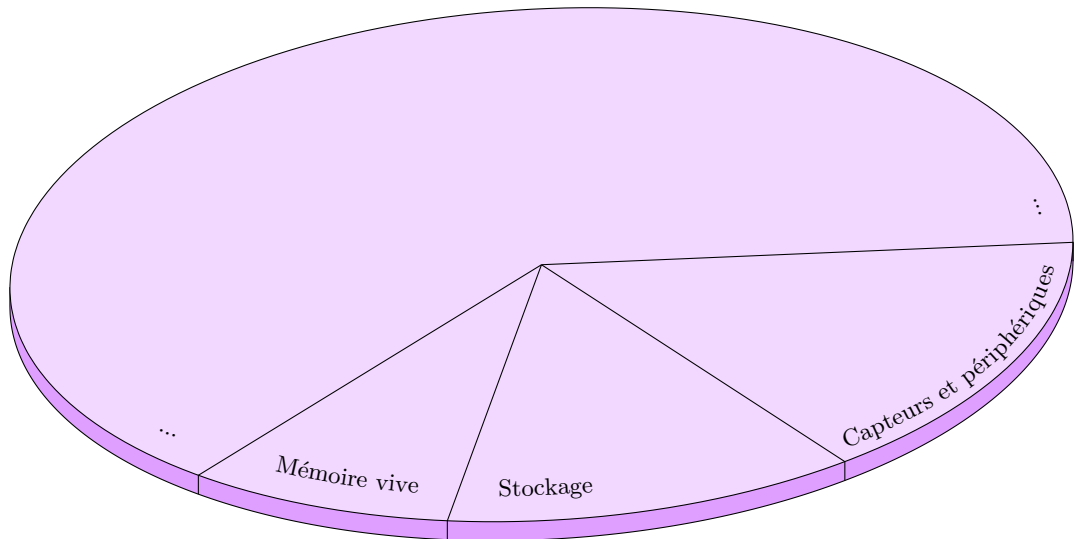
Sécurité dans Android

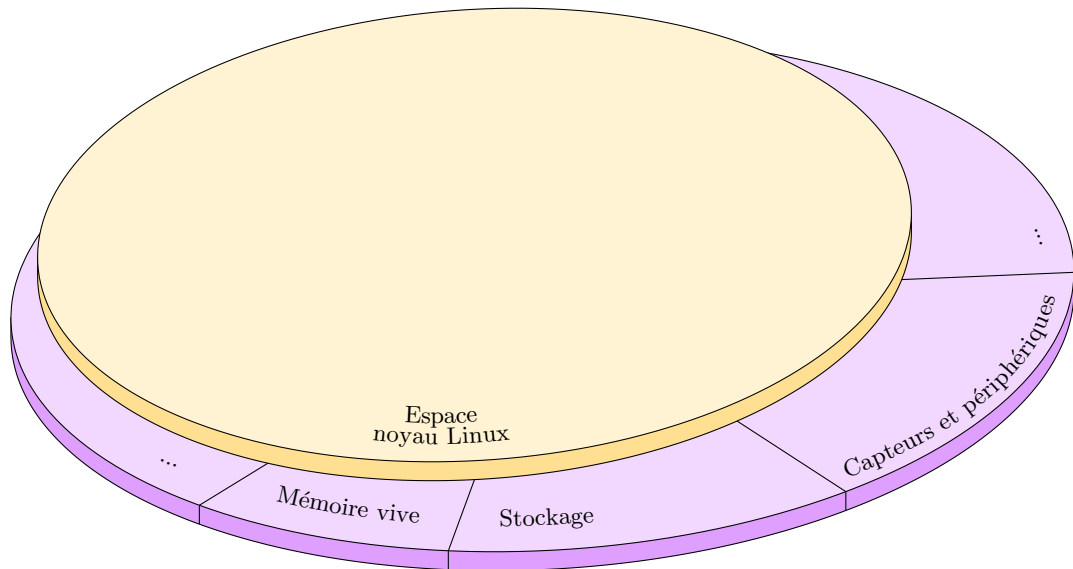
- Applications dangereuses pour le système

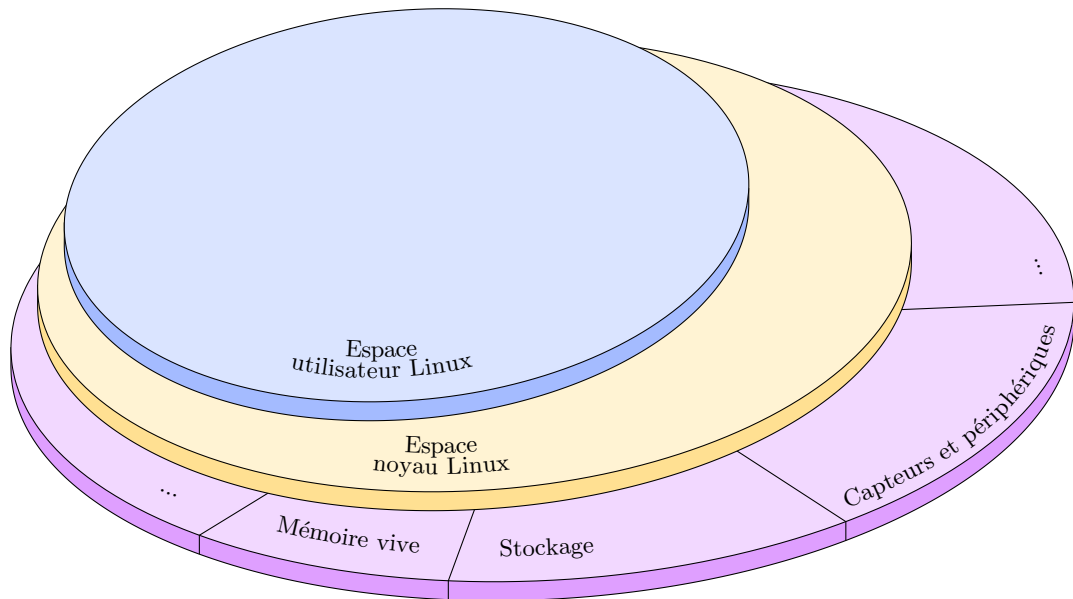
- Applications dangereuses pour le système
- Applications dangereuses pour l'utilisateur

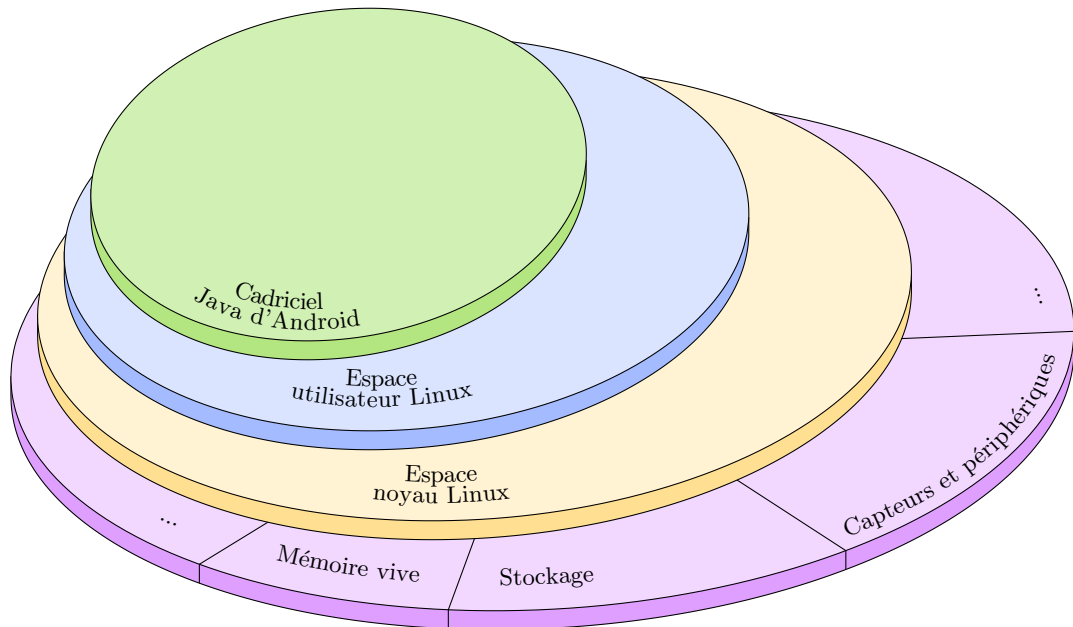
- Applications dangereuses pour le système
- Applications dangereuses pour l'utilisateur
- Applications jugées indésirables selon des critères moraux ou sociétaux

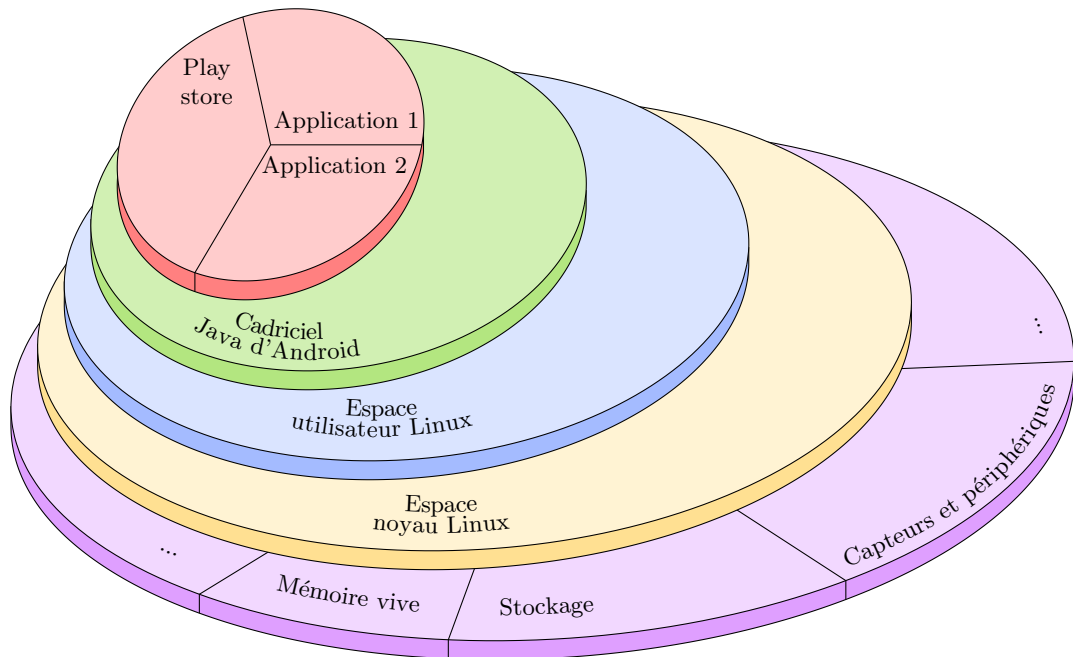
- Applications dangereuses pour le système
- Applications dangereuses pour l'utilisateur
- Applications jugées indésirables selon des critères moraux ou sociétaux

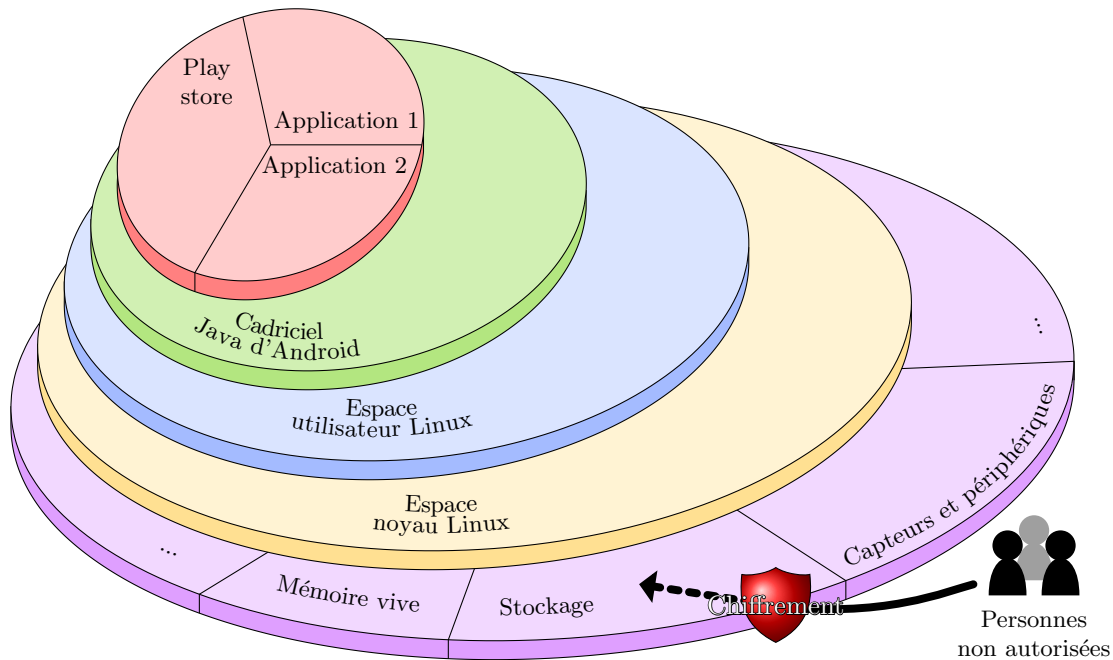




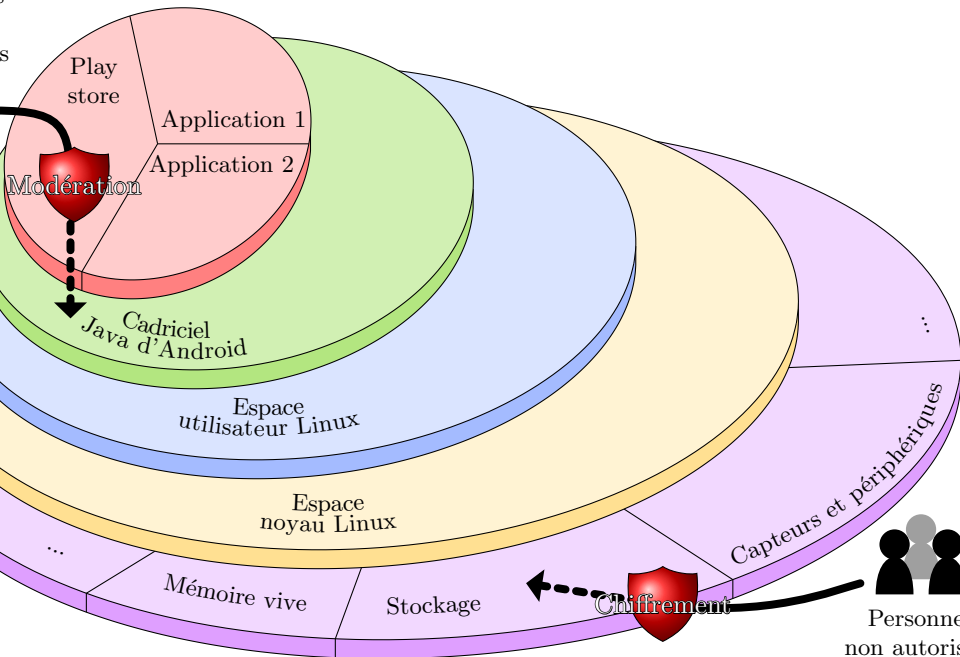






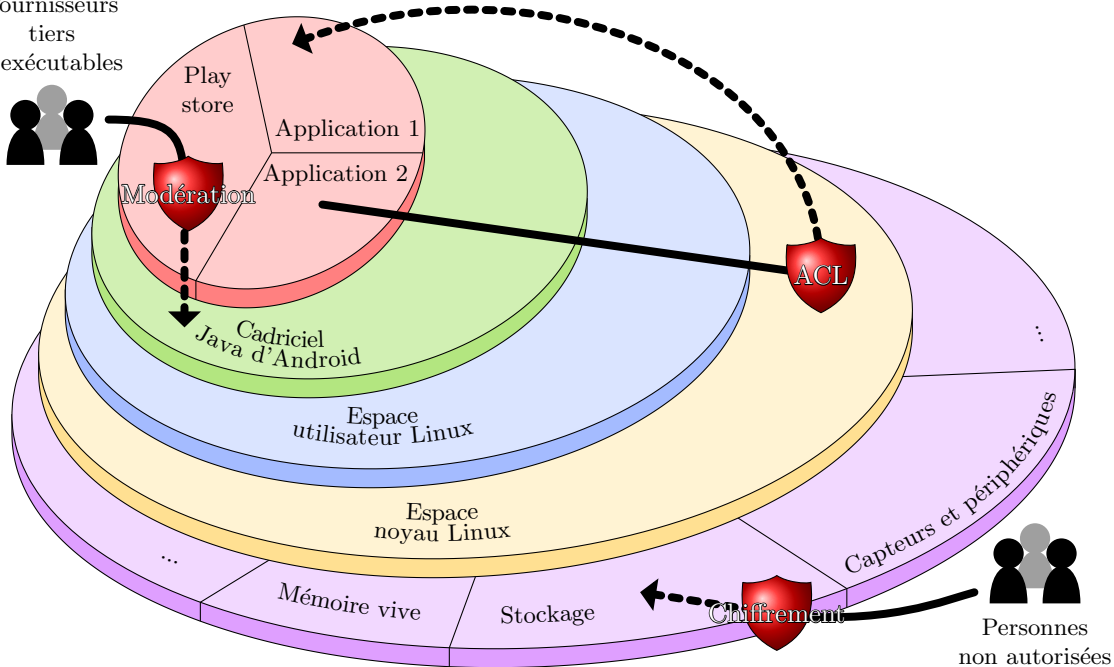


Fournisseurs
tiers
d'exécutables

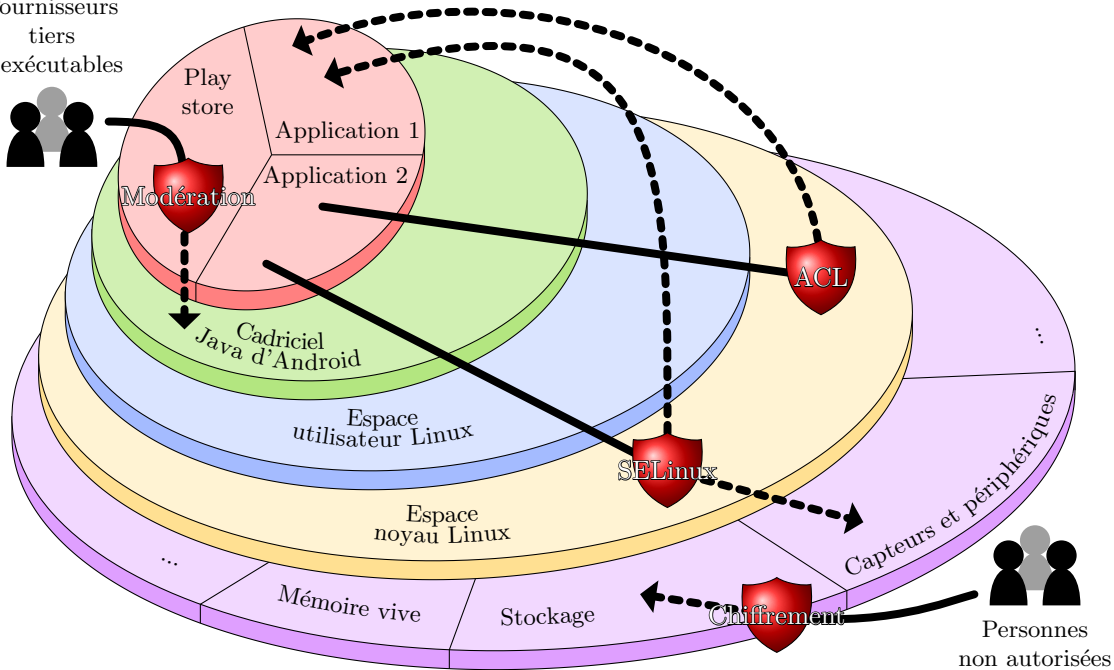


Personnes
non autorisées

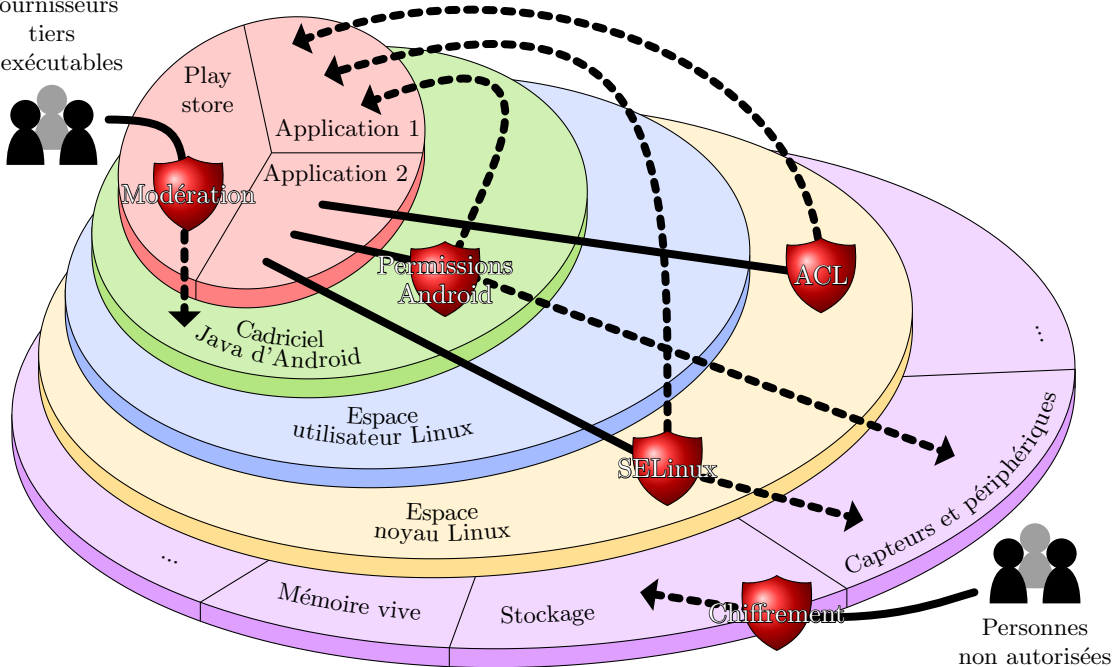
Fournisseurs
tiers
d'exécutables



Fournisseurs
tiers
d'exécutables



Fournisseurs
tiers
d'exécutables



Contributions

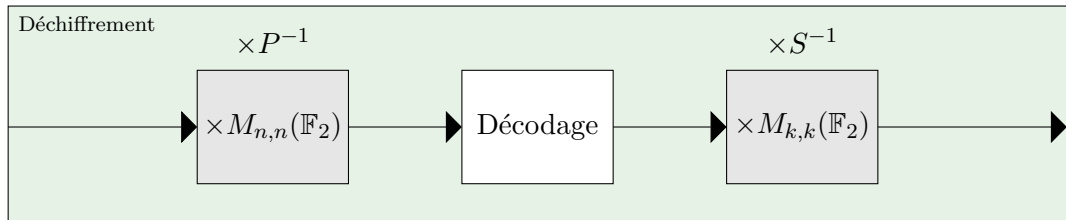
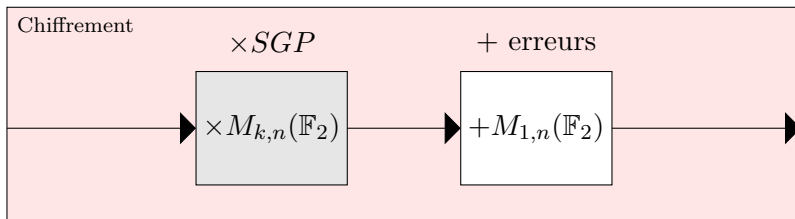
Cryptosystème de McEliece en environnement ouvert

*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]



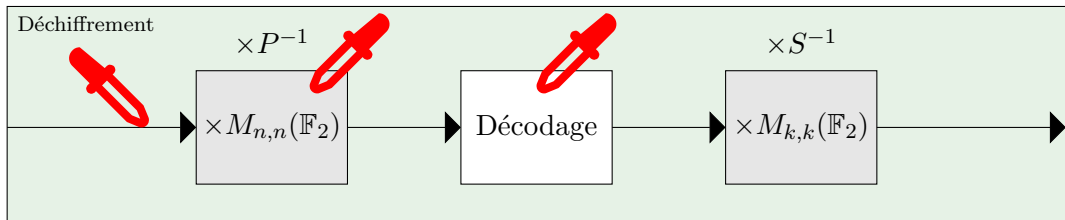
- Codes de Goppa

- 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

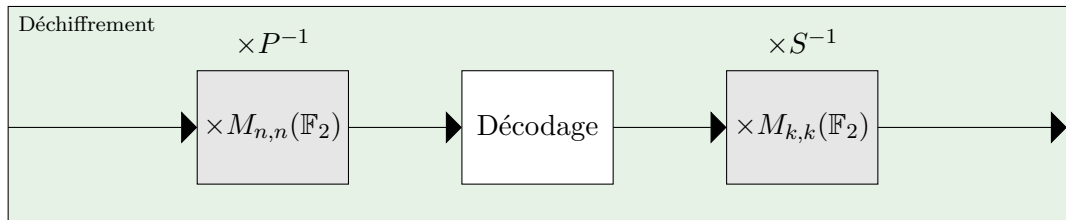
- Codes de Goppa
- ~~Codes de Reed-Solomon généralisés [SS92]~~
- ~~Codes de Reed-Muller [MS07]~~
- ~~Codes géométriques algébriques [FM08 ; CMP14]~~
- ~~Codes Bose-Chaudhuri-Hocquenghem [OTD10]~~
- ~~Codes alternants quasi-cycliques et alternants quasi-dyadiques [Fau+10]~~
- Codes sur \mathbb{F}_q [COT17]

- 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]

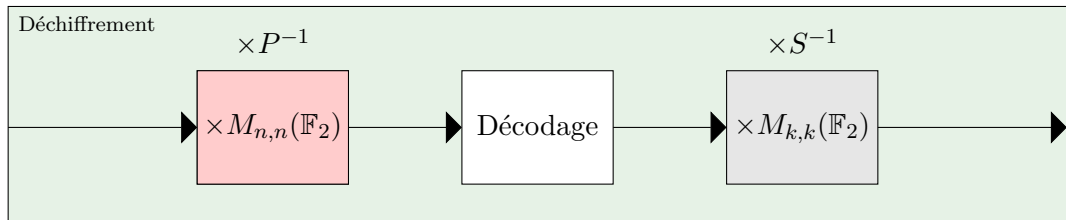
[Sho+10 ; Str11a ; Str+08 ; Str10 ; Ava+10 ; Str11b ; Mol+11 ; Che+14 ; VG14 ; HMP10]



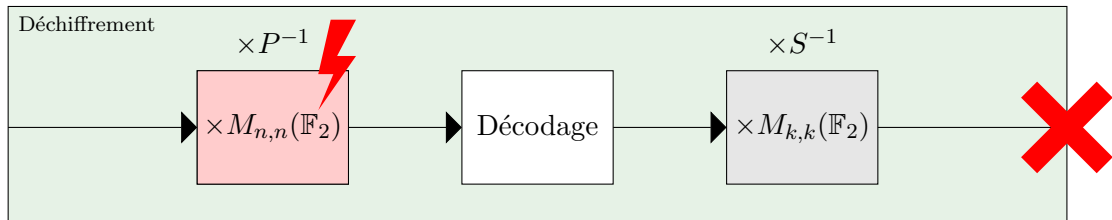
- Matrice de permutation P
- Code correcteur
- Matrice de mélange S



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

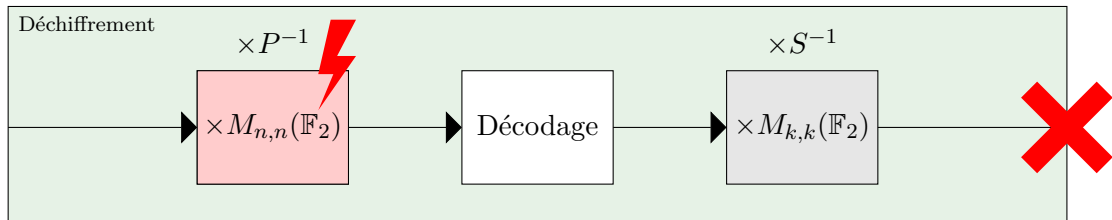


- Matrice de permutation P
- Code correcteur
- Matrice de mélange S



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

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



$$\times \begin{bmatrix} 0010111101111000010000101110 \\ 0111101001111110110111011 \\ 1100010000011001100000111 \\ 1000100100110010111000010 \\ 1110111011000111111010100 \\ 001011111010100001111010 \\ 101010001000010010110111 \\ 000011001111111101010111 \\ 111011000001011000110100 \\ 011101111011000010011010 \\ 101010011011011001000101 \\ 0001010111111110100110000 \\ 001010101101000101101111 \\ 0101101110100011111011100 \\ 0100111011111110000010111 \\ 001010001110101011011110 \\ 100101100101011100111000 \\ 011111101011001101110011 \\ 000000100110100000010000 \\ 001111000001000111111011 \\ 010110111111010110111010 \\ 001100011000100110111010 \\ 1101001101000111101100101 \\ 110101011101011111011101 \end{bmatrix}$$

$$\begin{bmatrix} 001000001000000100000001 \end{bmatrix} \begin{bmatrix} 11010101010001100000110000 \end{bmatrix}$$

$$\times \begin{bmatrix} 00101110 & 11100001 & 00010110 \\ 01111010 & 01111101 & 10111011 \\ 11000100 & 00110011 & 00000111 \\ 10001001 & 00110010 & 11100010 \\ 11101101 & 10001111 & 11010100 \\ 00101111 & 10101000 & 01111010 \\ 10101000 & 10000100 & 10110111 \\ 00001100 & 11111111 & 01010111 \\ 11101100 & 00010110 & 00110100 \\ 01110111 & 10110000 & 10011010 \\ 10101001 & 10110110 & 01000101 \\ 00010101 & 11111101 & 00110000 \\ 00101010 & 11010001 & 01101111 \\ 01011011 & 10100011 & 11011100 \\ 01001110 & 11111100 & 00010111 \\ 00101000 & 11101010 & 11011110 \\ 10010110 & 01010111 & 00111000 \\ 01111110 & 10110011 & 01110011 \\ 00000010 & 01101000 & 00010000 \\ 00111100 & 00010001 & 11111011 \\ 01011011 & 11110101 & 10111010 \\ 00110001 & 10001001 & 10111010 \\ 11010011 & 01000111 & 01100101 \\ 11010101 & 11010111 & 11011101 \end{bmatrix}$$

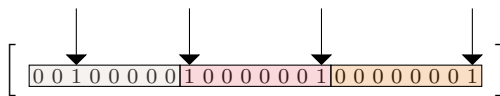
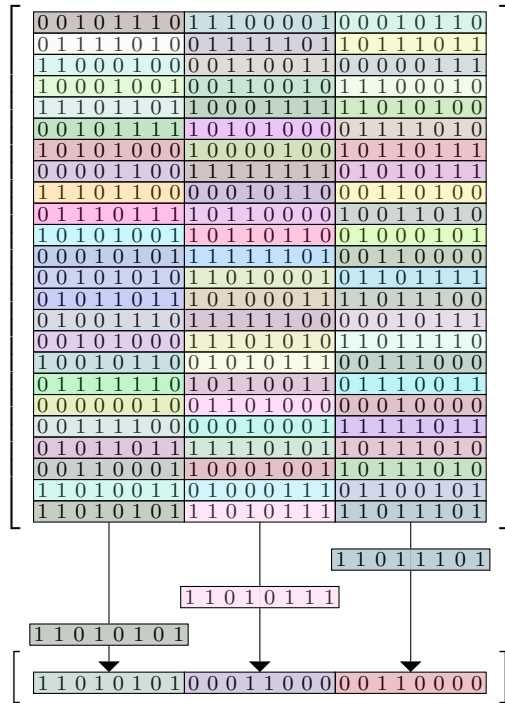
$$\begin{bmatrix} 00100000 & 10000001 & 00000001 \end{bmatrix}$$

$$\begin{bmatrix} 11010101 & 00011000 & 00110000 \end{bmatrix}$$

$$\times \begin{bmatrix} 00101110 & 11100001 & 00010110 \\ 01111010 & 01111101 & 10111011 \\ 11000100 & 00110011 & 00000111 \\ 10001001 & 00110010 & 11100010 \\ 11101101 & 10001111 & 11010100 \\ 00101111 & 10101000 & 01111010 \\ 10101000 & 10000100 & 10110111 \\ 00001100 & 11111111 & 01010111 \\ 11101100 & 00010110 & 00110100 \\ 01110111 & 10110000 & 10011010 \\ 10101001 & 10110110 & 01000101 \\ 00010101 & 11111101 & 00110000 \\ 00101010 & 11010001 & 01101111 \\ 01011011 & 10100011 & 11011100 \\ 01001110 & 11111100 & 00010111 \\ 00101000 & 11101010 & 11011110 \\ 10010110 & 01010111 & 00111000 \\ 01111110 & 10110011 & 01111001 \\ 00000010 & 01101000 & 00010000 \\ 00111100 & 00010001 & 11111011 \\ 01011011 & 11110101 & 10111010 \\ 00110001 & 10001001 & 10111010 \\ 11010011 & 01000111 & 01100101 \\ 11010101 & 11010111 & 11011101 \end{bmatrix}$$

$$\begin{bmatrix} 00100000 & 10000001 & 00000001 \end{bmatrix}$$

$$\begin{bmatrix} 11010101 & 00011000 & 00111000 \end{bmatrix}$$


 \times


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 :

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

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

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

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

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

$$n = 9$$

$$p = 3$$

$$t = 4$$

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

$$n = 9$$

$$p = 3$$

$$t = 4$$

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

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

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

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

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

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

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

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

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

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

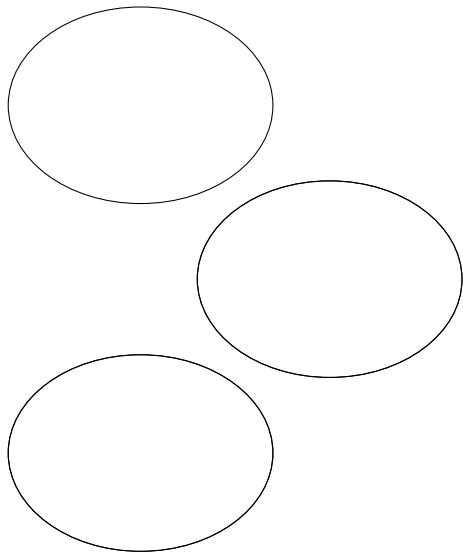
Les lignes 1, 7 et 8 ont
forcément leurs uns respectifs
dans des groupes de colonnes
différents

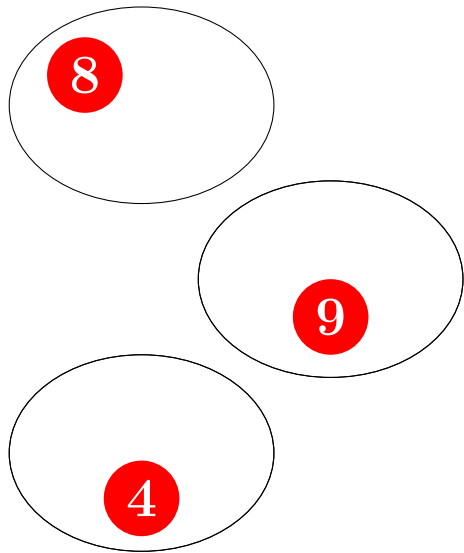
$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 &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

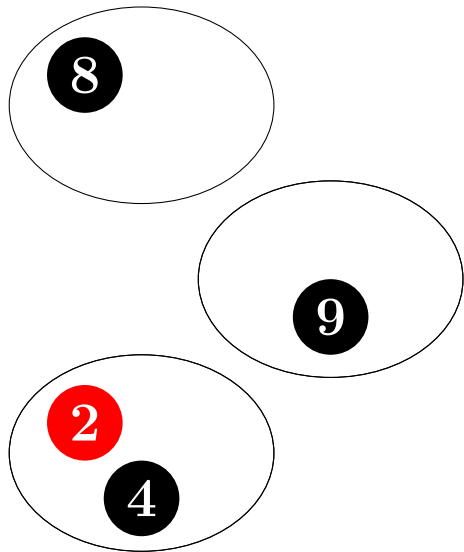
$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 &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

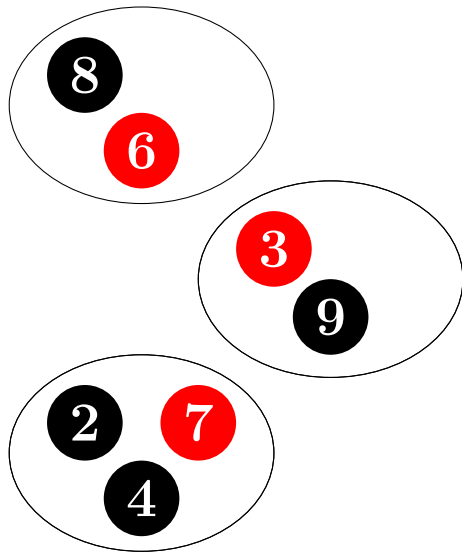
Les lignes 2, 8 et 9 ont
forcément leurs uns respectifs
dans des groupes de colonnes
différents

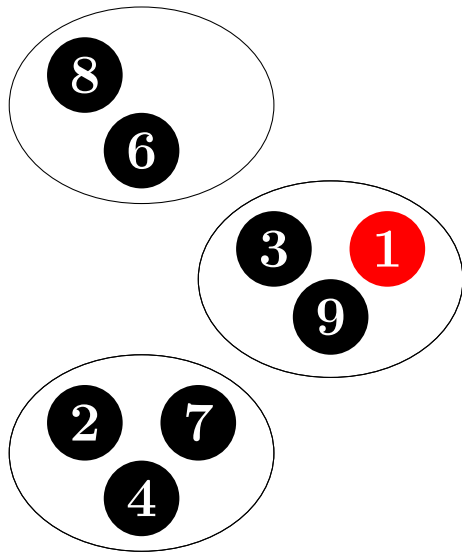
$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 &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

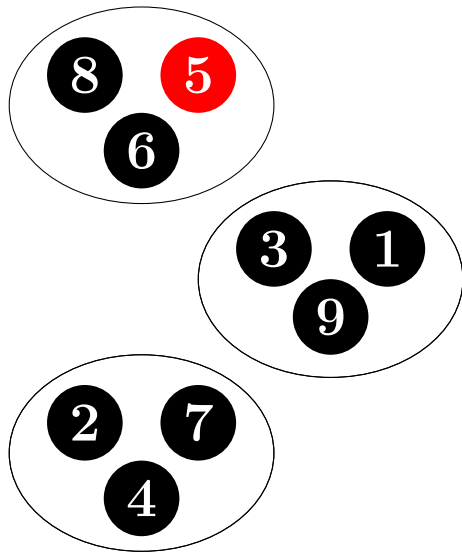


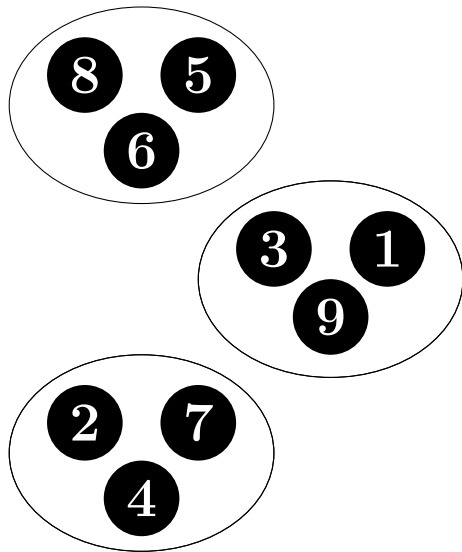




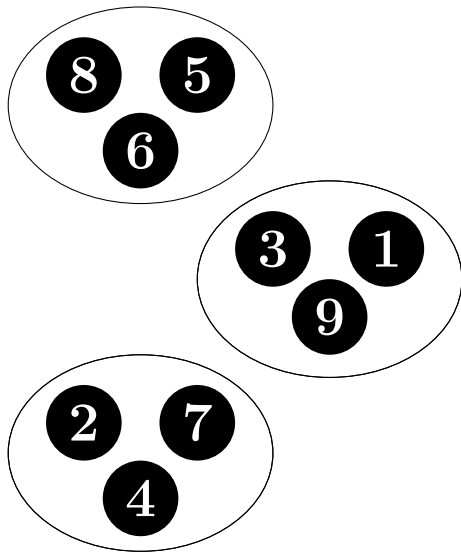




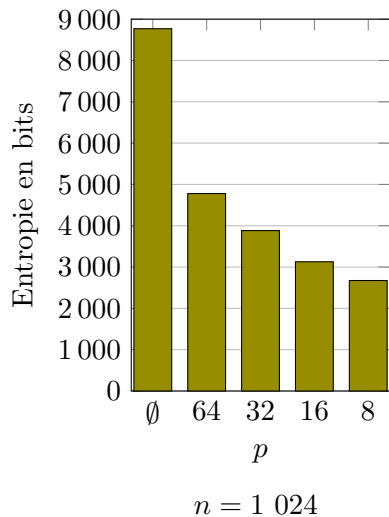


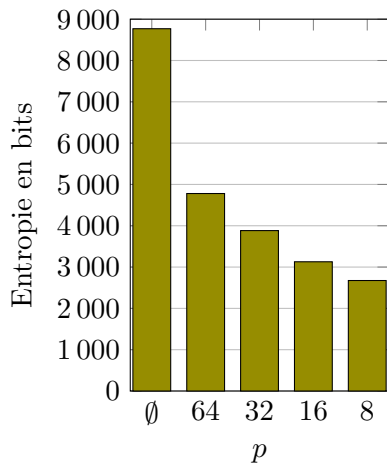
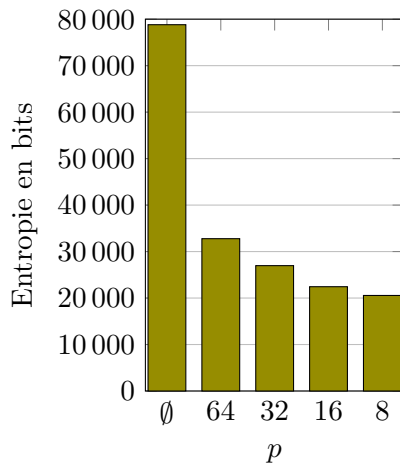


$$\begin{bmatrix}
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\
 \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\
 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & \mathbf{1} & 0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



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



 $n = 1\ 024$  $n = 6\ 960$

~~Autoprotection de ses propres exécutables~~

~~Autoprotection de ses propres exécutables~~

Bénéficiaire 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

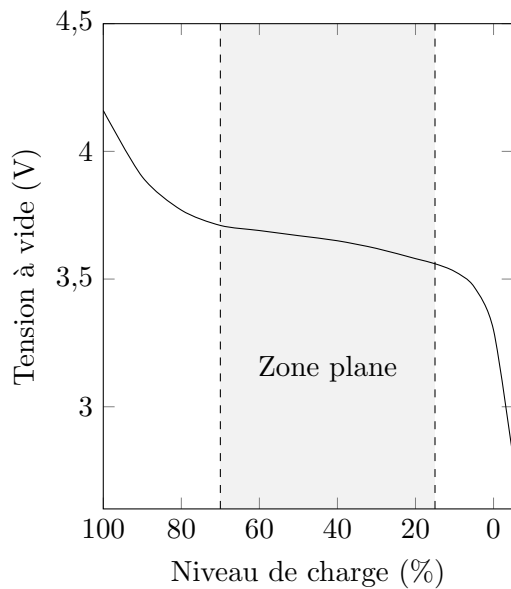
- Autonomie de la batterie plus longue
- Durée de vie de la batterie plus longue
- Température de fonctionnement moins élevée
- Durée de charge plus courte

- 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

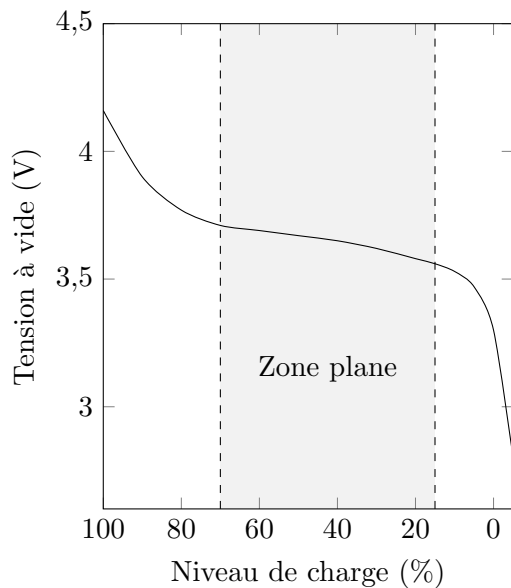
- Autonomie de la batterie plus longue
- Durée de vie de la batterie plus longue
- Température de fonctionnement moins élevée
- Durée de charge plus courte
- Réduction des risques
- Optimisation des matières premières

- 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

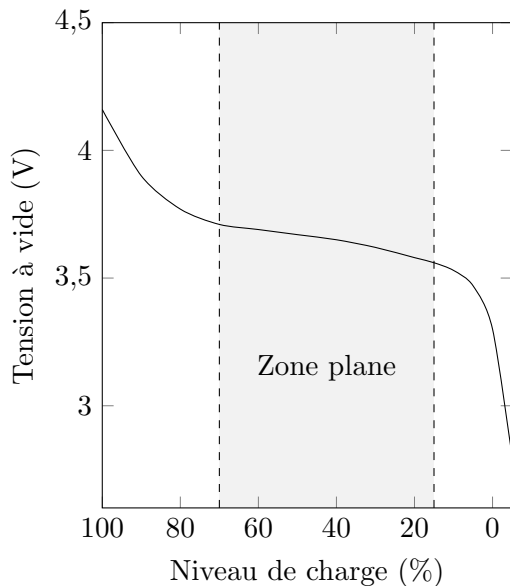
- Comportement non linéaire



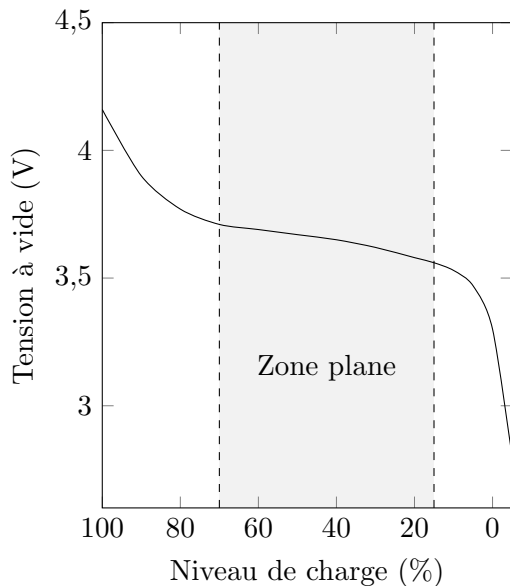
- Comportement non linéaire
- Contraintes de mesure du signal



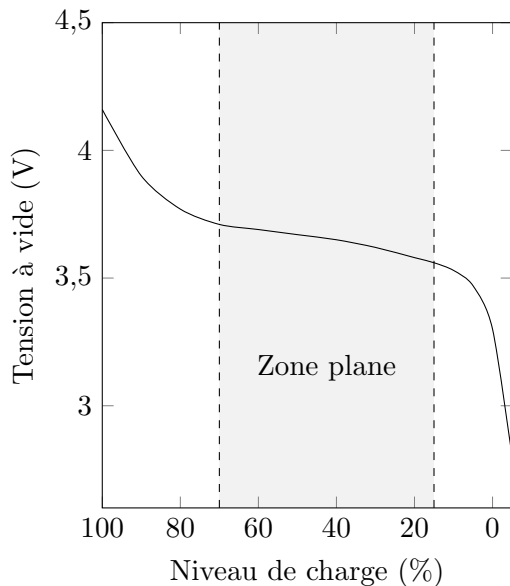
- Comportement non linéaire
- Contraintes de mesure du signal
- Comportement dépendant de :
 - la température de fonctionnement



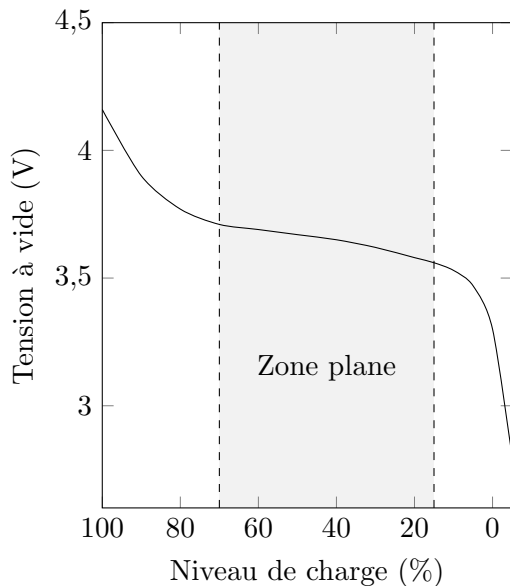
- Comportement non linéaire
- Contraintes de mesure du signal
- Comportement dépendant de :
 - la température de fonctionnement
 - l'âge de la batterie



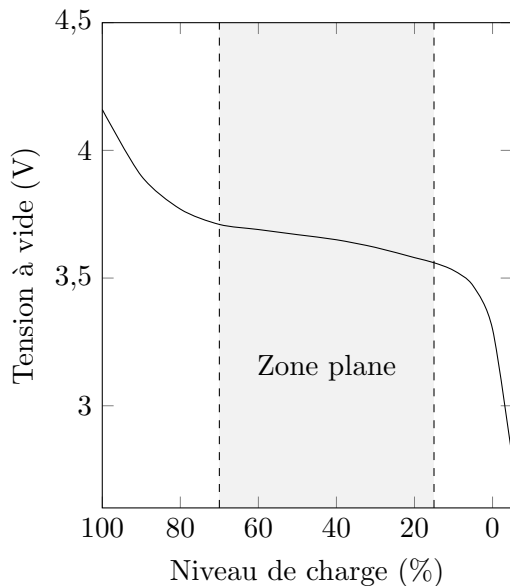
- Comportement non linéaire
- Contraintes de mesure du signal
- Comportement dépendant de :
 - la température de fonctionnement
 - l'âge de la batterie
 - la qualité des ressources utilisées



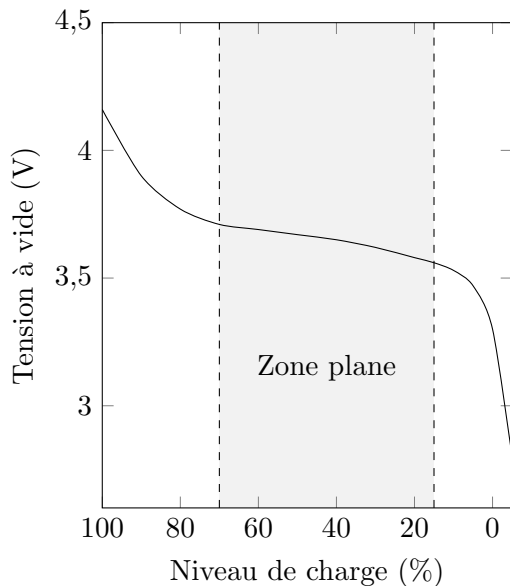
- Comportement non linéaire
- Contraintes de mesure du signal
- Comportement dépendant de :
 - la température de fonctionnement
 - l'âge de la batterie
 - la qualité des ressources utilisées
 - leur utilisation



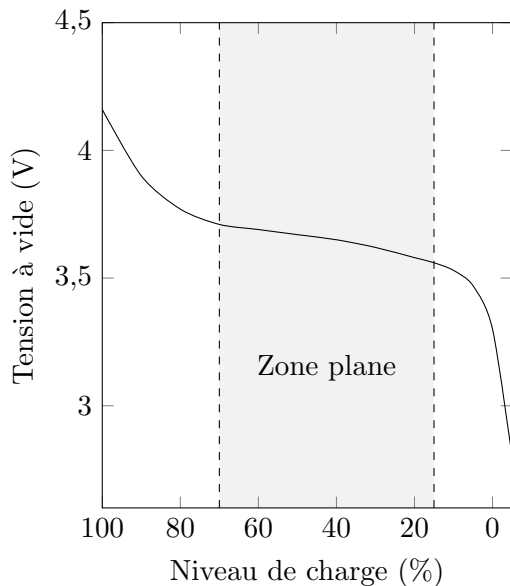
- Comportement non linéaire
- Contraintes de mesure du signal
- Comportement dépendant de :
 - la température de fonctionnement
 - l'âge de la batterie
 - la qualité des ressources utilisées
 - leur utilisation
- Risque de combustion voir d'explosion



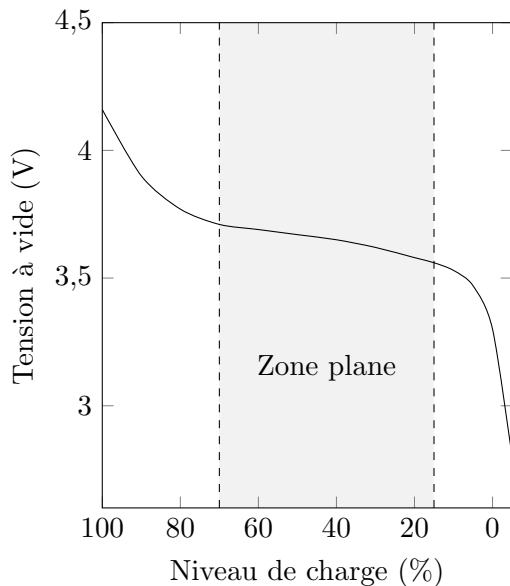
- Comportement non linéaire
- Contraintes de mesure du signal
- Comportement dépendant de :
 - la température de fonctionnement
 - l'âge de la batterie
 - la qualité des ressources utilisées
 - leur utilisation
- Risque de combustion voir d'explosion
- Déséquilibres entre les cellules

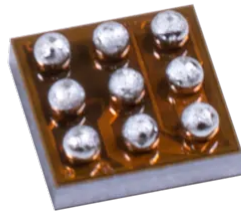
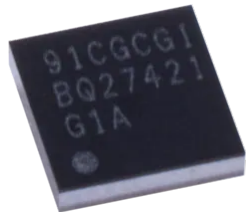


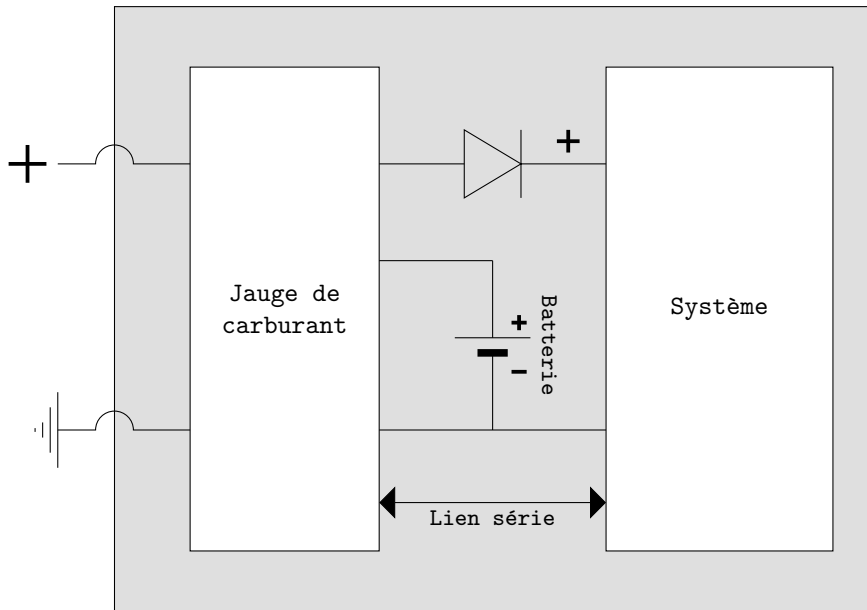
- Comportement non linéaire
- Contraintes de mesure du signal
- Comportement dépendant de :
 - la température de fonctionnement
 - l'âge de la batterie
 - la qualité des ressources utilisées
 - leur utilisation
- Risque de combustion voir d'explosion
- Déséquilibres entre les cellules
- Charge intelligente

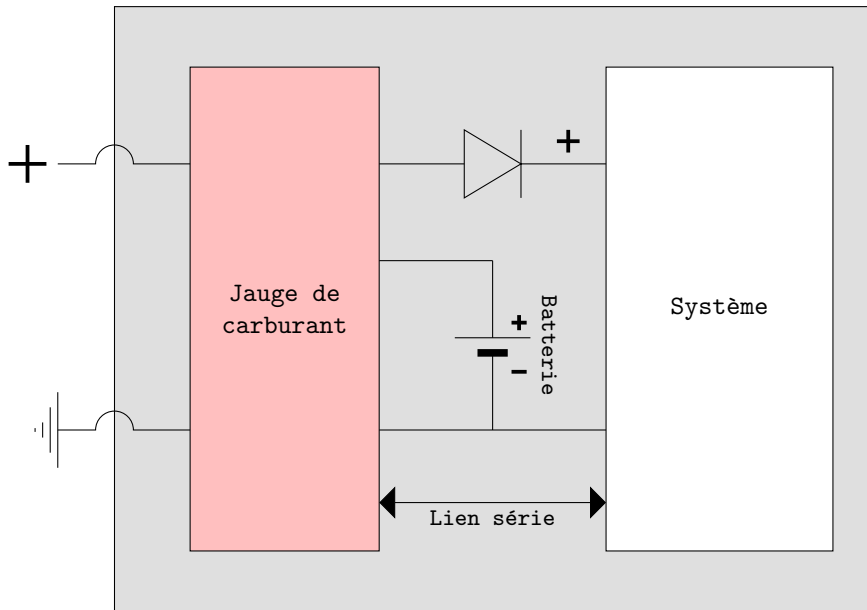


- Comportement non linéaire
- Contraintes de mesure du signal
- Comportement dépendant de :
 - la température de fonctionnement
 - l'âge de la batterie
 - la qualité des ressources utilisées
 - leur utilisation
- Risque de combustion voir d'explosion
- Déséquilibres entre les cellules
- Charge intelligente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









- 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

BACKGROUND_SERVICE

FOREGROUND_SERVICE

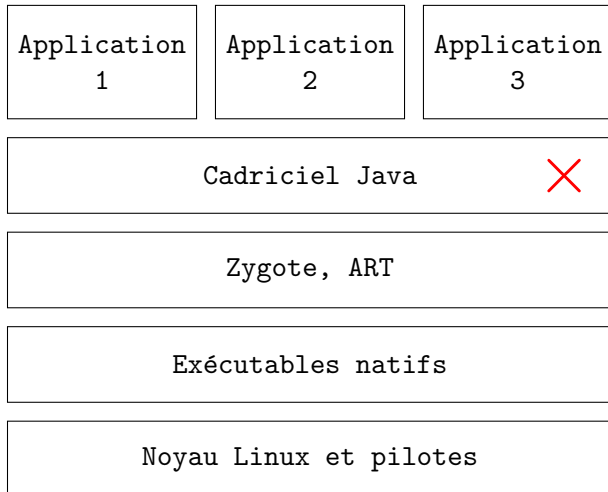
HIGH_SAMPLING_RATE_SENSORS

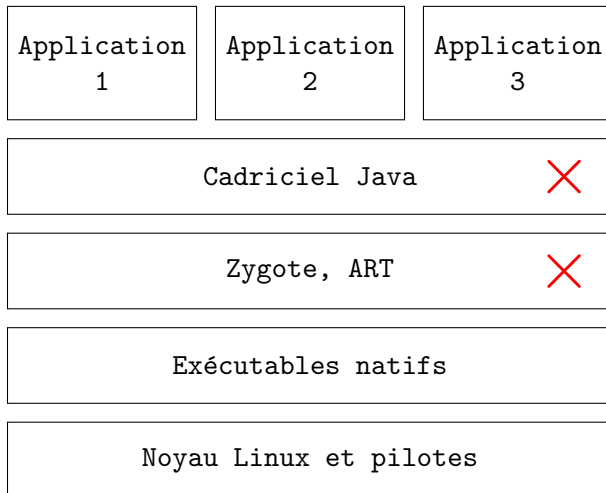
- Santé de la batterie
 - Statut de charge
 - Source de charge
 - Courant instantané
 - Capacité
 - Température
 - Tension
 - Niveau de charge
 - Compteur d'énergie
- FOREGROUND_SERVICE
- HIGH_SAMPLING_RATE_SENSORS

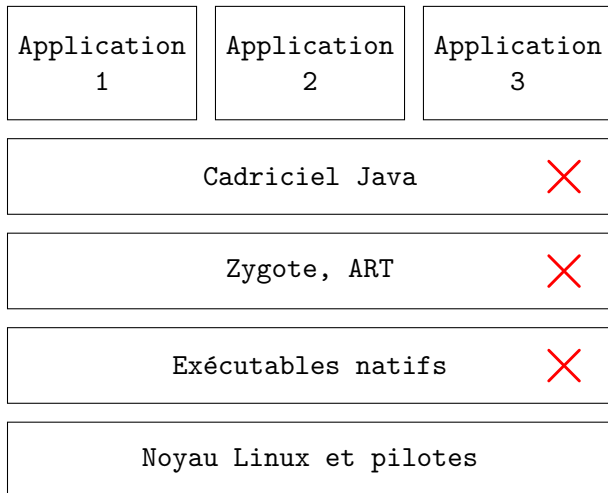
```

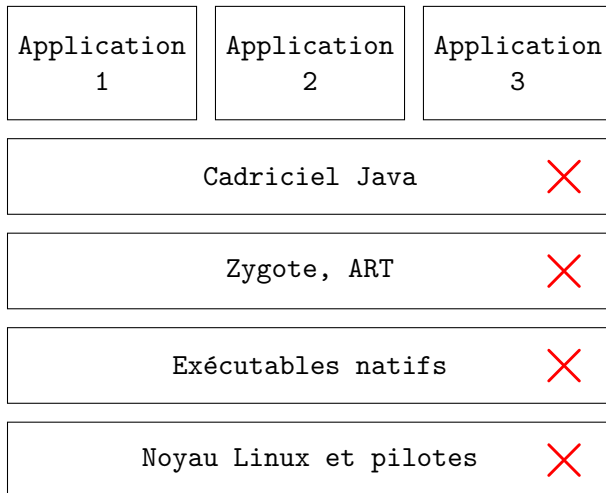
/**
 * Checks if a sensor should be capped according to HIGH_SAMPLING_RATE_SENSORS permission.
 * [...]
 */
private boolean isSensorInCappedSet(int sensorType) {
    return (sensorType == Sensor.TYPE_ACCELEROMETER
        || sensorType == Sensor.TYPE_ACCELEROMETER_UNCALIBRATED
        || sensorType ==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

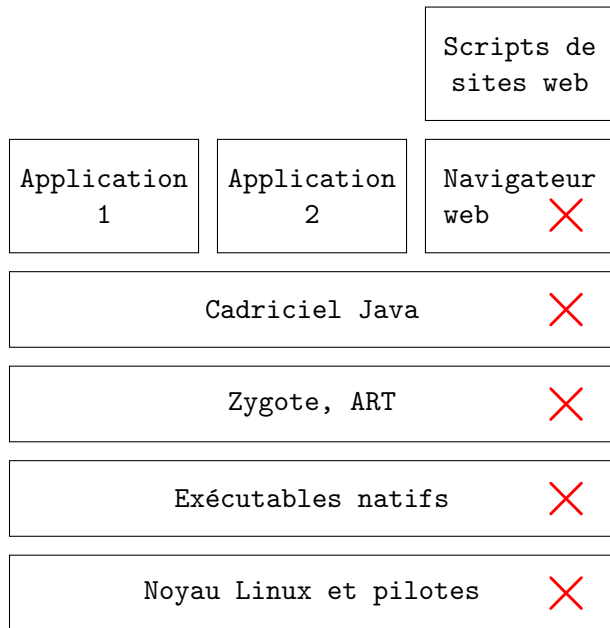
```

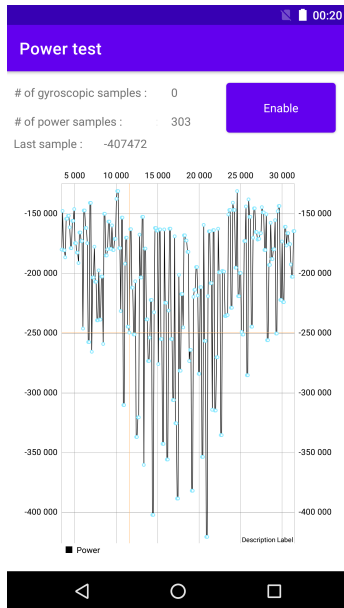


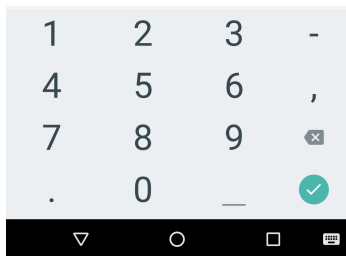
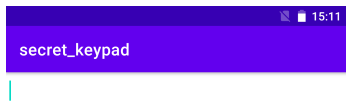


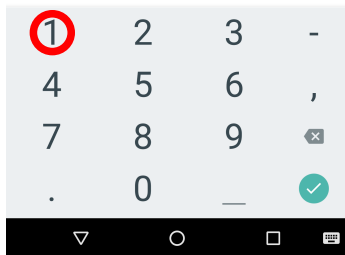
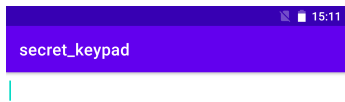


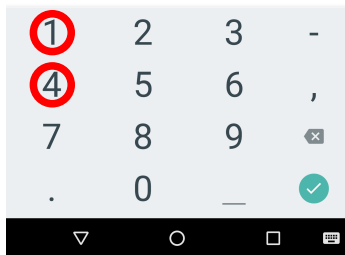
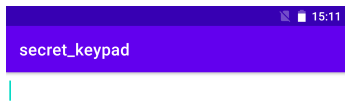


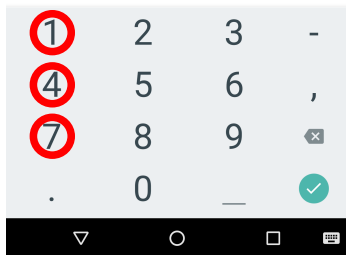
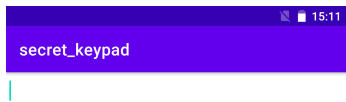


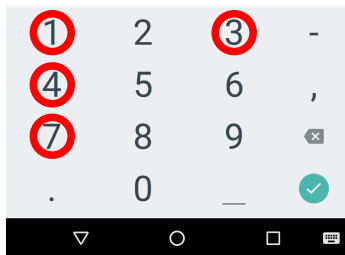
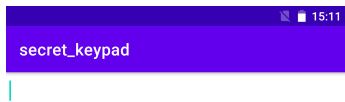


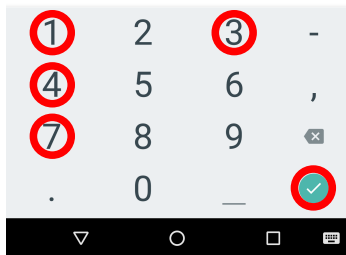
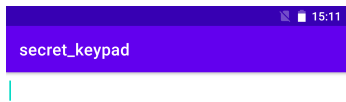


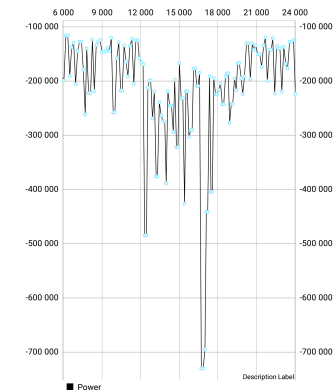
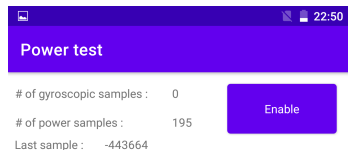
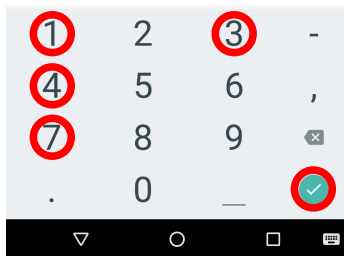
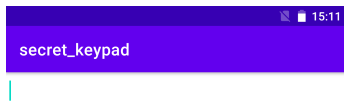


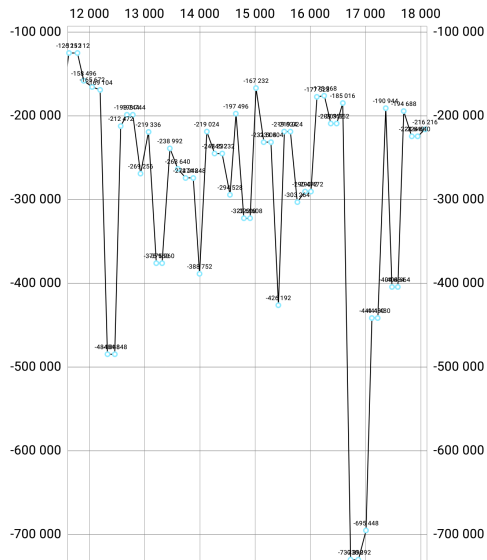
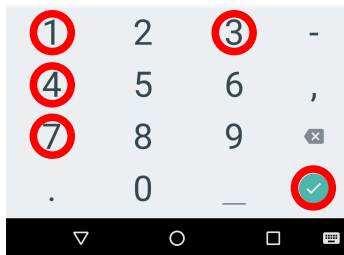
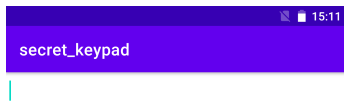


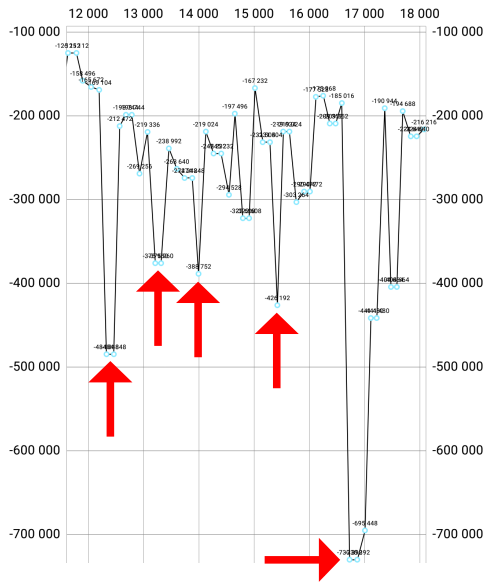
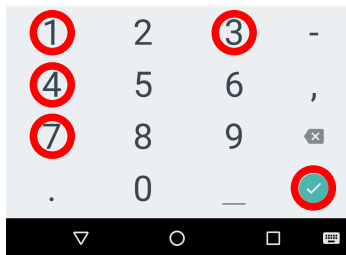
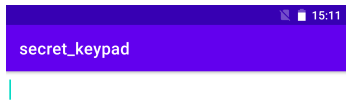


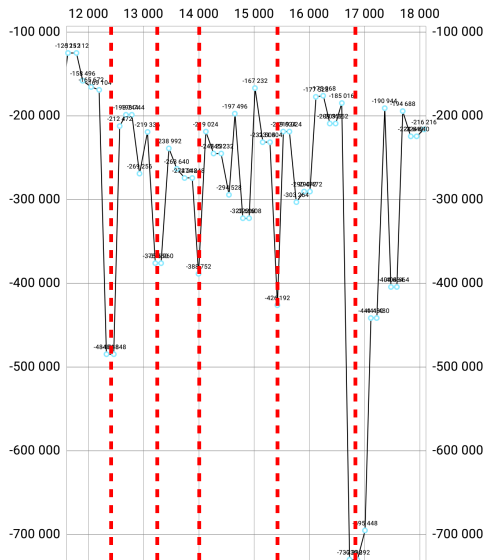
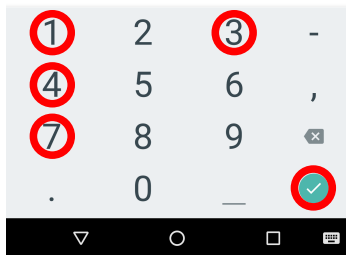
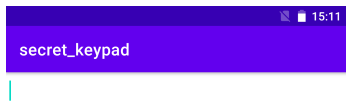


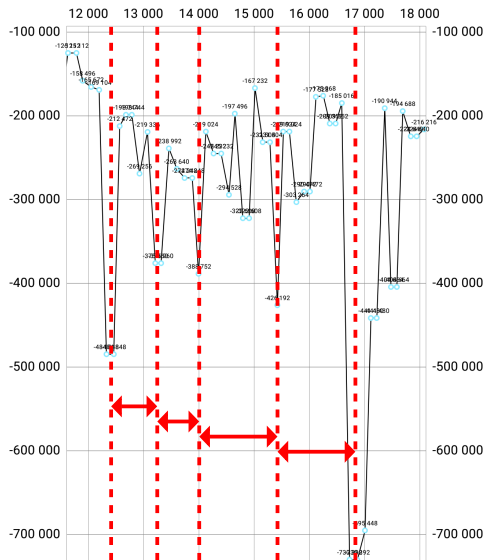
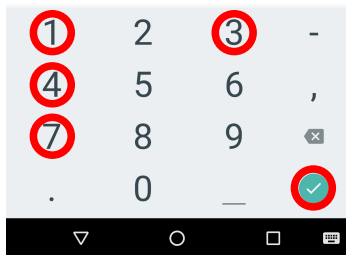
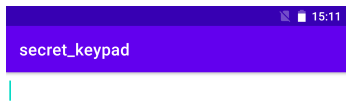


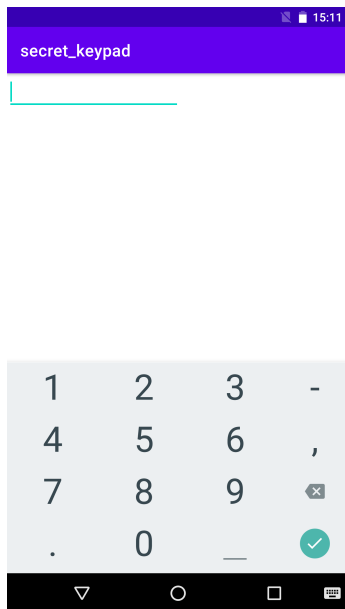


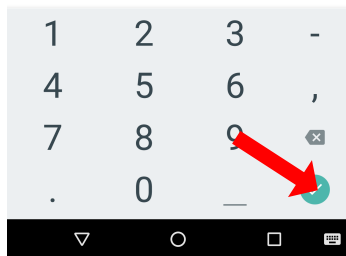
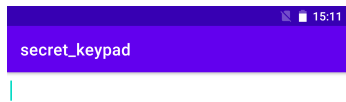


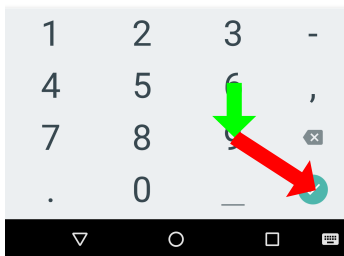
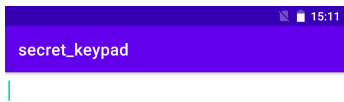


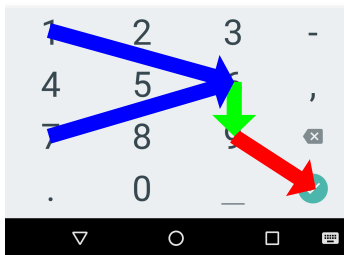
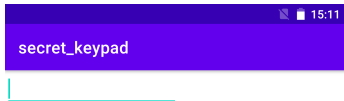


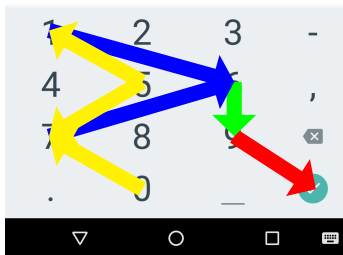
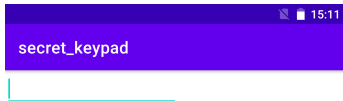




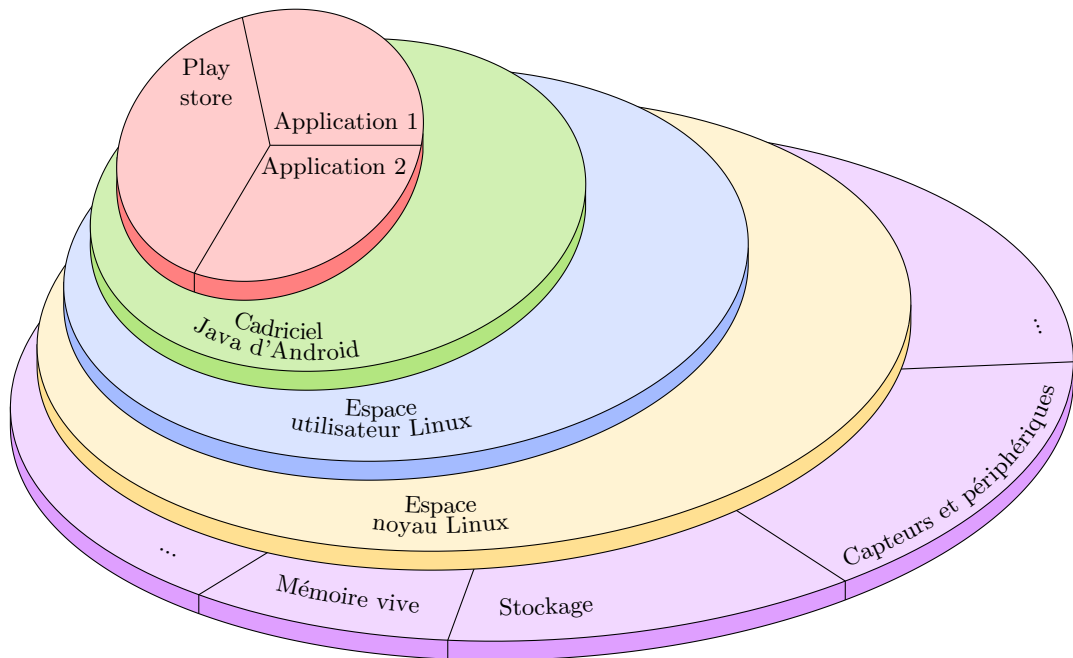


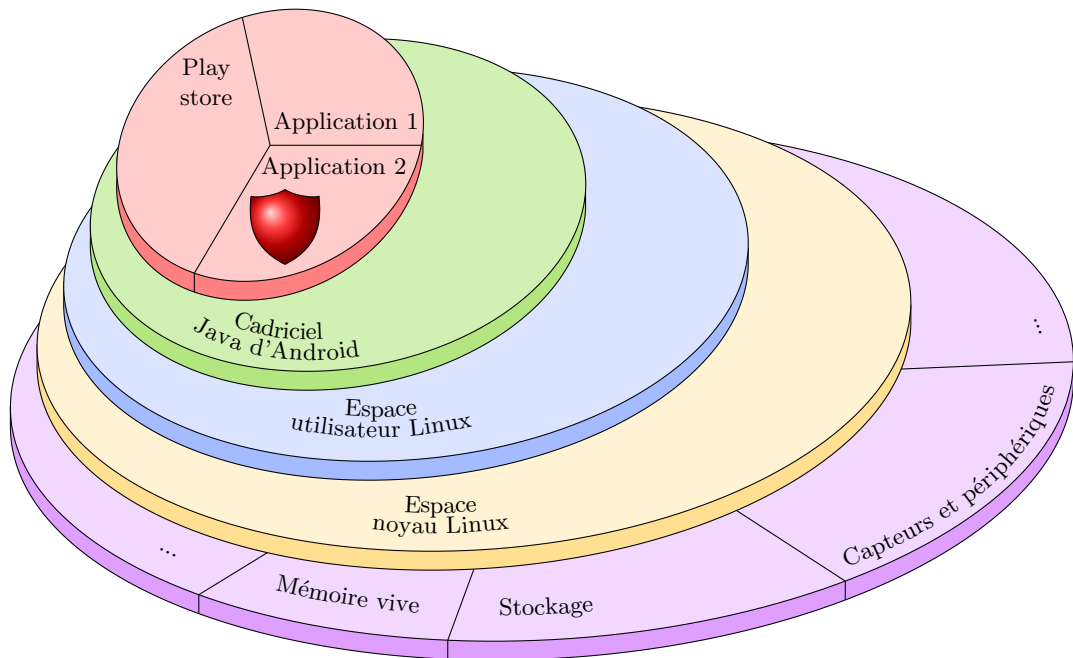


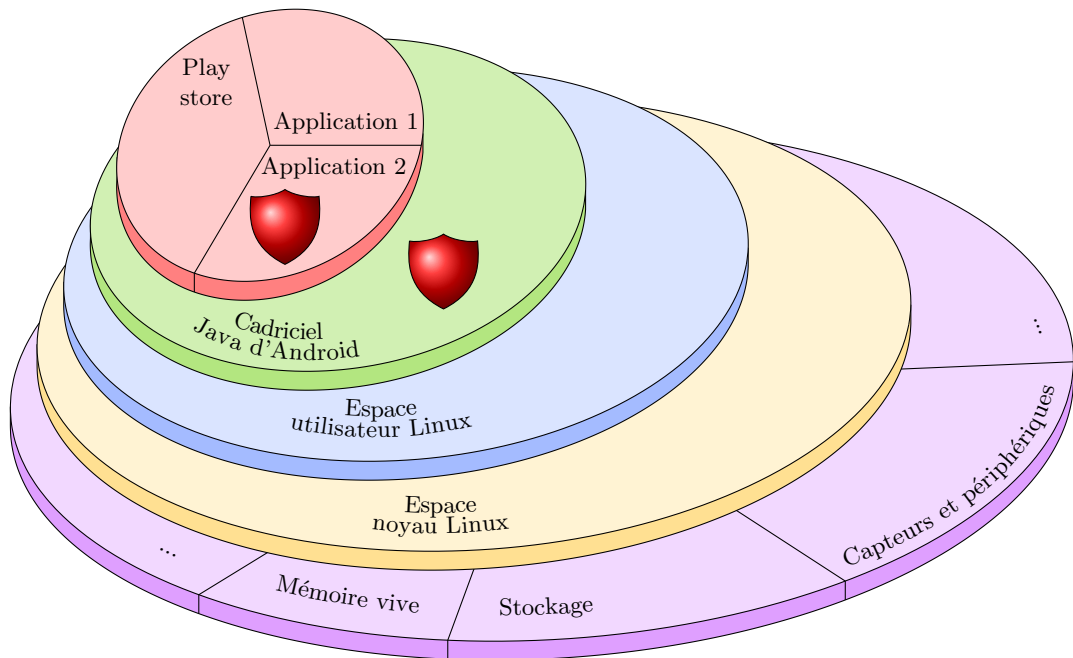




```
1 (arbre '(3.37 4.01 1 1) (cons '(10) '()) 0)  
2 => ((((((10 3 7 4 7) (10 3 7 4 1))))))
```

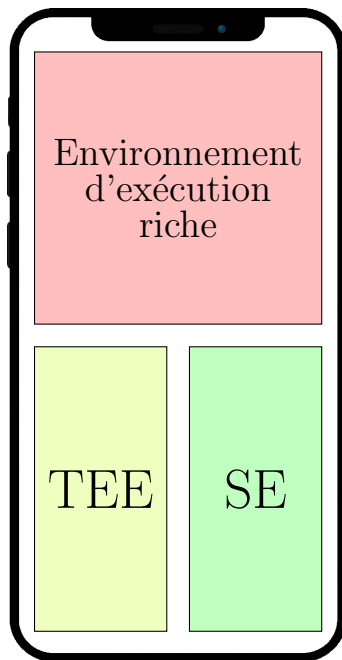
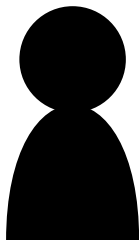





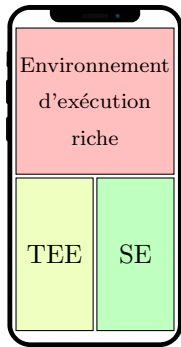


Propositions

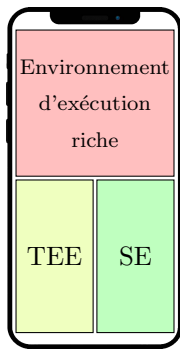
Utilisateur et
propriétaire de
la plateforme



Utilisateur et
propriétaire de
la plateforme



Utilisateur et
propriétaire de
la plateforme



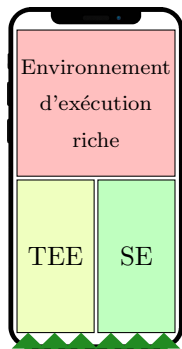
Entreprise C

Association D

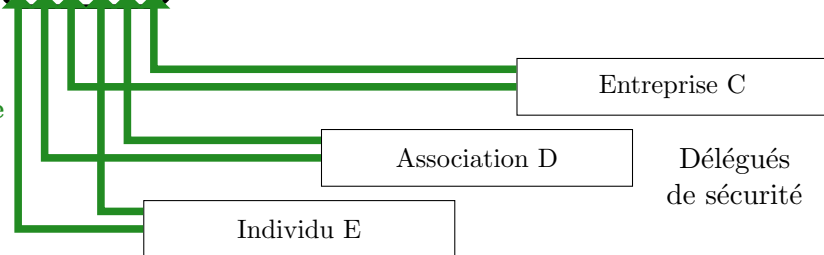
Délégués
de sécurité

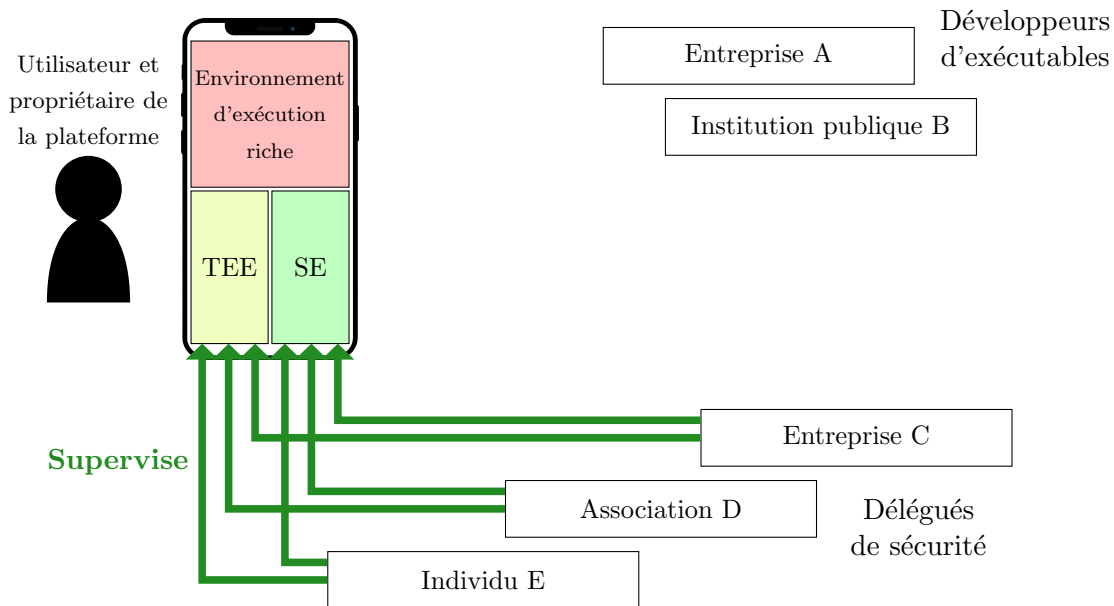
Individu E

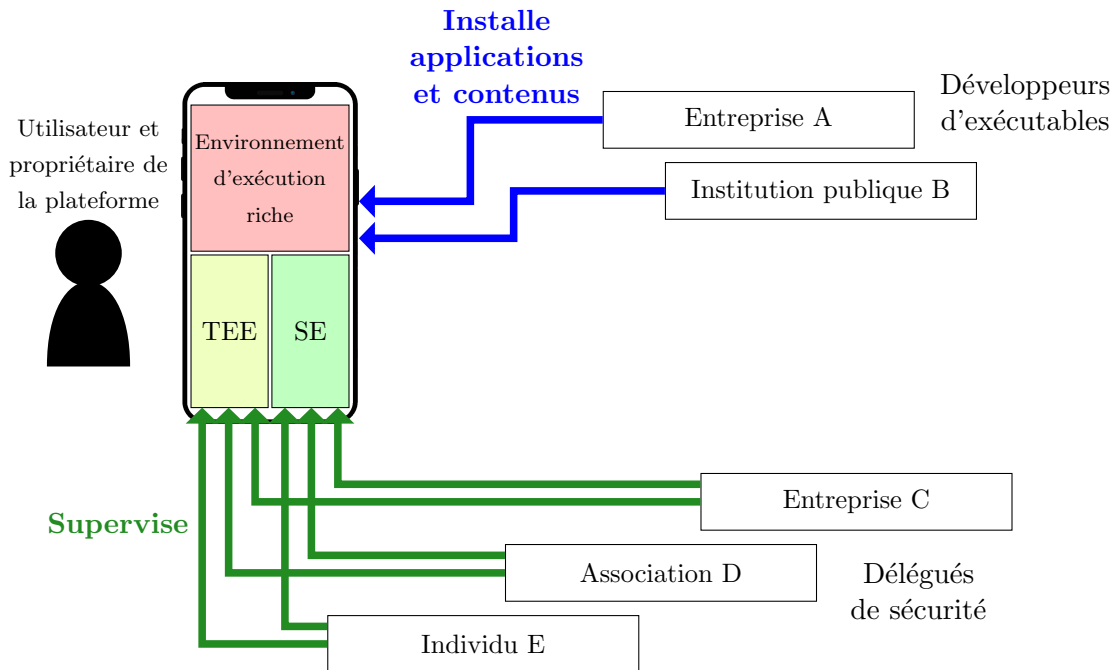
Utilisateur et
propriétaire de
la plateforme

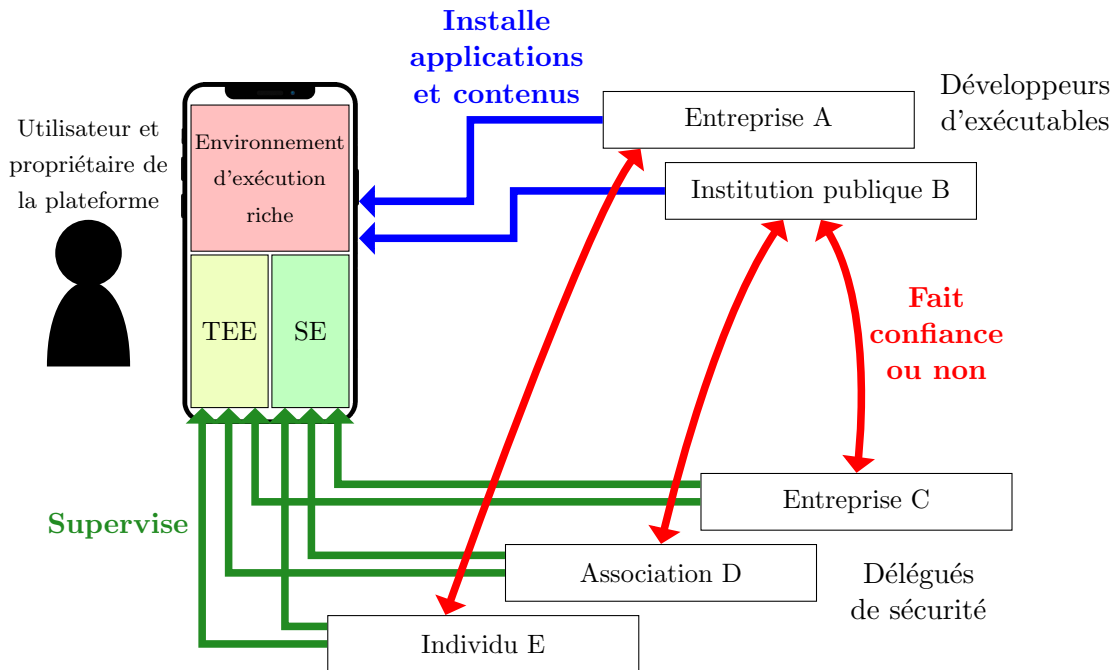


Supervise





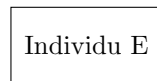
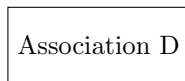
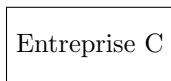




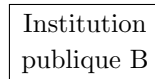
Constructeurs
de composants
sécurisés



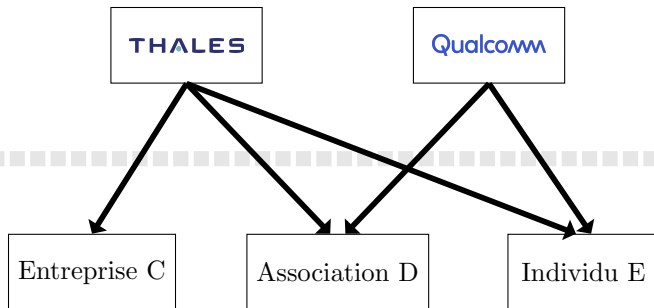
Délégués
de sécurité



Développeurs
d'exécutables



Constructeurs
de composants
sécurisés



Délégués
de sécurité

Signe et
embarque les
certificats

Développeurs
d'exécutables

Entreprise A

Institution
publique B

Constructeurs
de composants
sécurisés

THALES

Qualcomm

Délégués
de sécurité

Entreprise C

Association D

Individu E

Signe et
embarque les
certificats

Développeurs
d'exécutables

Entreprise A

Institution
publique B

Modère et signe
les exécutables
et contenus

Constructeurs

de cor
séc



Dé
de s



Déve
d'exécutables



GSMA™

ne et
rque les
ificats

e et signe
cutables
ntenus

publique D

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 TILICH. "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 Algebraic 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 TILICH 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.