Chaire C3S – Présentation

- Inaugurée le 5 octobre 2017
- Première journée de la chaire le 15/01/2019
- Un comité de pilotage, un comité opérationnel et 5 axes de recherche
- 18 enseignants-chercheurs de Télécom Paris sur 3 départements
  - Informatique & Réseaux
  - Communications & Électronique
  - Sciences Économiques et Sociales
- Co-directions des thèses avec les industriels
- 7 doctorants, 5 postdoctorants

RENAULT THALES

Valeo
SMART TECHNOLOGY FOR SMARTER CARS

NOKIA

WAVESTONE

FONDATION Mines-Télécom
La Fondation de l'IMT

SÉCURITÉ ROUTIÈRE TOUS RESPONSABLES

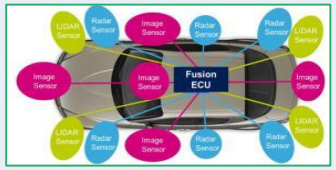
www.telecom-paris.fr/c3S

Contexte et objectifs (2017-2023)
Coopération, Connectivité & Automatisation

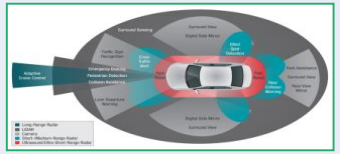
La connectivité augmente les surfaces d'attaque

- **Les surfaces d'attaque évoluent et se complexifient**
- **Les cas d'usage augmentent les surfaces d'attaque**
- **La cybersécurité concerne un écosystème global impliquant une interopérabilité interentreprises, inter-acteurs, ….et donc inter-systèmes**
- **Approche pluridisciplinaire et multicouches**

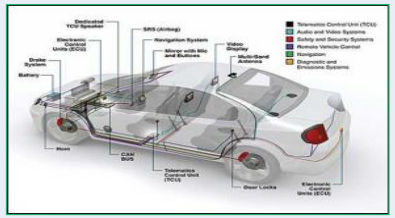
- **Combinaison de technologies d'accès sans-fil**
  - ITS-G5 (IEEE 802.11p)/3G/4G/5G/Bluetooth/Wi-Fi, USB, OBD II,.GNSS, ….
- **Diversité des modes de communications**
  - Vehicle-to-Anything (V2X)
  - V2V, V2I, I2V, V2N, N2V, V2S, V2C, V2P
- **Diversité des protocoles**
- **Cas d'usage ETSI C-ITS Day 1/2/3**



Capteurs

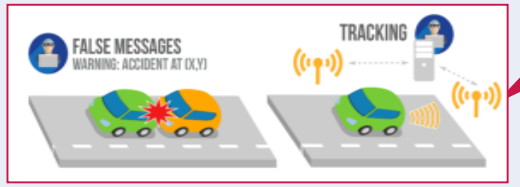


Perception



Communication (ECU, CAN bus, OBU, ..)

Interfaces multiples de communication



Faiblesses/Failles

Risques, vulnérabilités, menaces

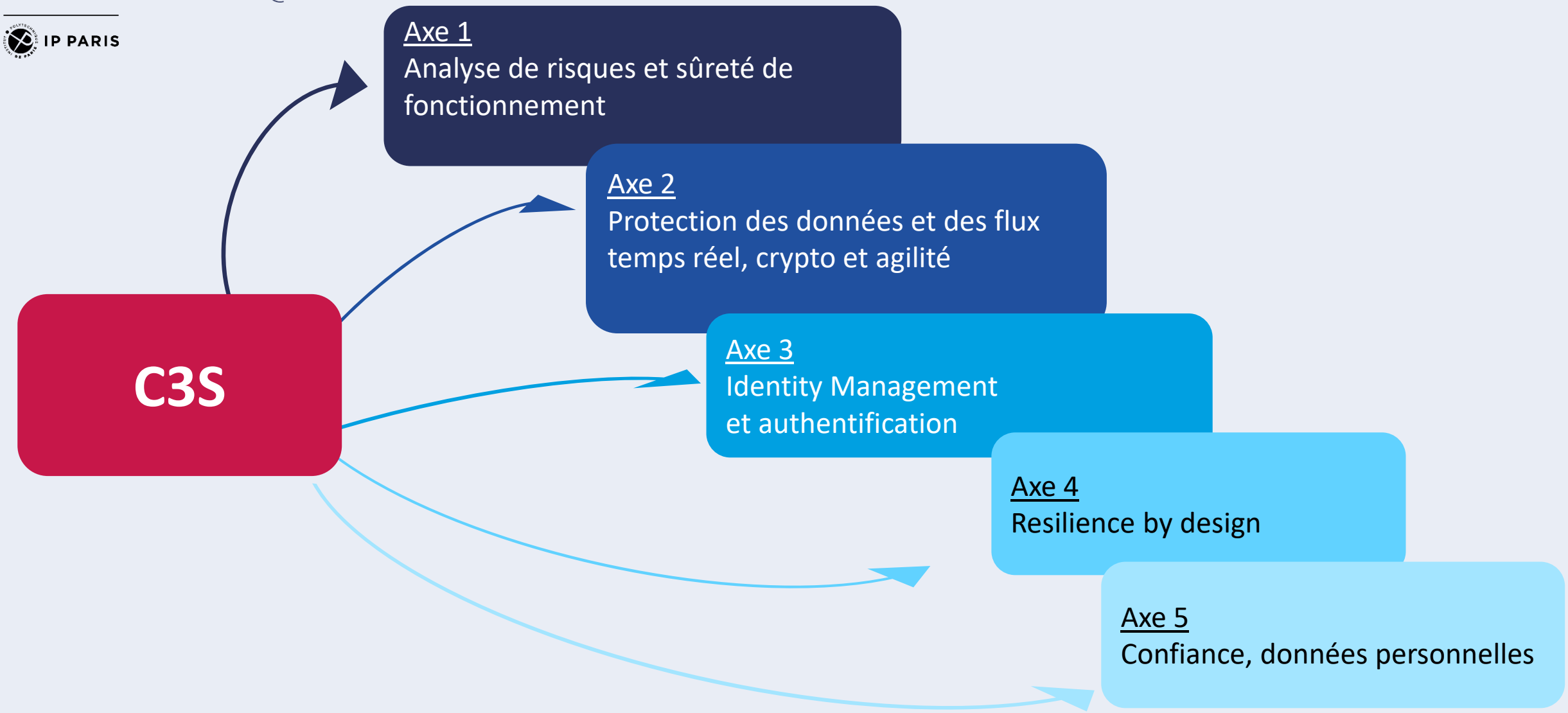
Cyberattaques

Comment sécuriser le VC/VCA?

Cadre réglementaire : national, européen et mondial (CNIL, ANSSI, CE, UNECE,RGPD, CCAM, NHTSA, ENISA...)

Standards ETSI/IEEE/ISO/CEN/IETF
Standards SAE, ISO/SAE 21434, ISO26262

Cinq axes de recherche



Axe 1
Analyse de risques & sûreté de fonctionnement

- **Animateurs**
  - JL. Danger (TP), P. Cincilla (Renault)

- **Objectifs**
  - Analyser et formaliser le risque de cyberattaques
    - Sur le véhicule (système embarqué)
    - Sur l'infrastructure (système débarqué)
  - Définir des contre-mesures et des solutions de cyberprotection
  - En lien avec la notion de sûreté de fonctionnement
- 2 Doctorants, 2 Postdocs

Deux thèses

Model-based Joint Analysis of Safety and Security

- **Problématique et approche**
  - Trouver un compromis, lors de la conception du système, entre les problématiques de sécurité et de sûreté, tout en considérant les contraintes de performance, de taille et de coût du système
- **Doctorante :** Sahar Berro
- **Encadrants :** L. Apvrille, G. Duc
- **Travaux passés et en cours**
  - Passés : Arbres d'attaque-défense améliorés en prenant en compte des notions d'architecture du système cible afin de permettre de sélectionner l'ensemble optimal de contre-mesures sous contraintes (sécurité uniquement)
  - En cours : Étude de l'impact des contre-mesures de sécurité sur la sûreté (et vice-versa)
- **Publications :** *International Workshop on Graphical Models for Security*, 2019.

Strategic and quantitative analysis for security risk assessment

- **Problématique et approche**
  - Proposer des outils et des méthodes d'aide à la décision pour l'évaluation des risques de sécurité basés sur des analyses quantitatives dans le cadre du véhicule connecté
    - Prise en compte des risques liés à la gestion de la chaîne logistique
    - Intégration dans les approches qualitatives classiques de gestion des risques comme définies dans ISO/IEC 27005
- **Doctorant :** Nicolas Van Cauter
- **Encadrants :** J. Leneutre, G. Memmi
- Thèse en cours de démarrage

Deux Postdocs

Model-based High-level Integration of Heterogenous Components

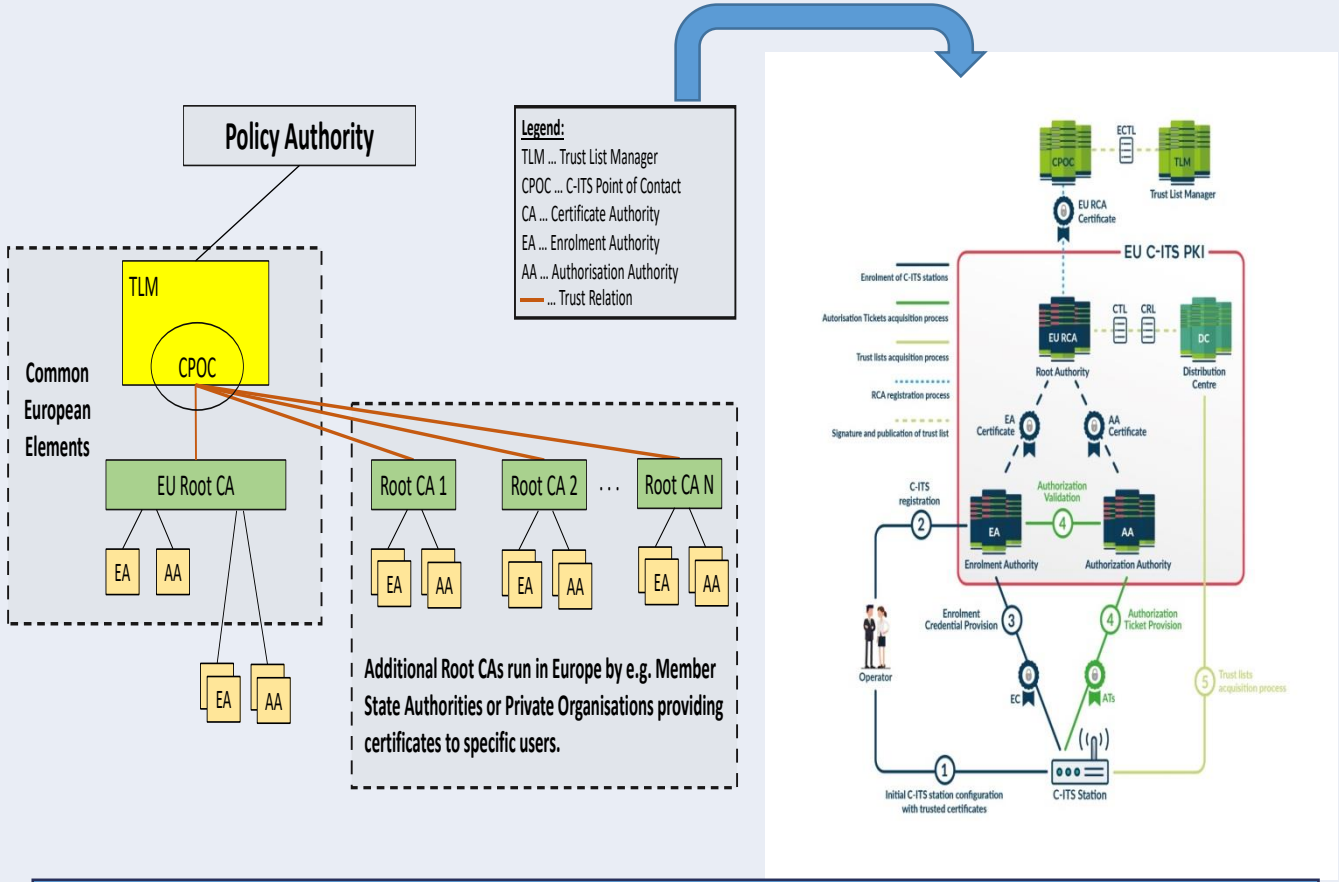
- **Problématique et approche**
  - Intégration de composants hétérogènes de façon sûre et sécurisée
  - Approche : technique d'agrégation de méta-modèles
- **PostDoc :** Skander Turki
- **Encadrants :** L. Apvrille, R. Ameur-Boulifa
- **Travaux en cours**
  - Début très récent (1er décembre 2020)
  - En cours : découverte de SysML-Sec

Decision support methods and tools for security hardening

- **Problématique et approche**
  - Proposer des méthodes et des outils d'aide à la décision pour traiter les risques de sécurité à base d'analyse quantitative
    - Prendre en compte les interactions entre les attaquants et les défenseurs
    - Garantir le meilleur compromis entre le niveau de sécurité atteint et les autres contraintes
- **Encadrant :** Jean Leneutre
- Sujet en recherche de candidat

Axe 2
Protection des données

- **Animateurs**
  - R. Khatoun (TP), R. Dubois (Thalès)
- **Contexte**
  - Protéger les informations (confidentialité, intégrité)
  - Infrastructure de confiance à clés publiques pour les messages V2X
  - Manque de flexibilité dans les standards sécurité (ETSI, IEEE) et limites des performances
- **Objectifs**
  - **Protection des flux de données**
    - **Cryptographie légère et robuste** adaptée à la faible puissance de calcul disponible dans certains calculateurs
    - **Cryptographie temps-réel** adaptée aux contraintes temps-réel de certains échanges
  - **Crypto-Agilité des protocoles**
    - **Cryptographie agile** permettant le remplacement dynamique et sécurisé des algorithmes et des paramètres
    - Nouvelle propriété pour les protocoles (dans le contexte d'attaque et le contexte normal)



C-ITS/CCAM Platform: EU trust model, EC Certificate Policy, Release 1
Certificats pseudonymes, signature numérique, ECDSA, ECIES

1 stage M2, 2 thèses de doctorat, 1 Postdoc (en cours de recrutement)

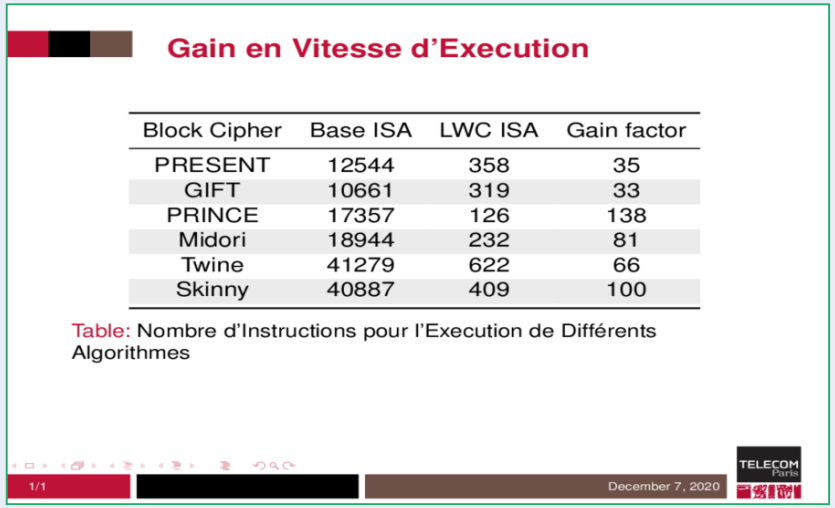
Cryptographic primitives adapted to connected cars requirements

- **Problématique & approche**
  - Etudier les architectures de cryptoprocesseurs pour la cryptographie légère afin de répondre à l'exigence d'agilité des voitures connectées
- **Doctorant :** Etienne Tehrani
- **Encadrants :** JL. Danger, T. Graba
- **Travaux réalisés**
  - Classification des algorithmes cryptographiques légers pour optimiser leur mise en œuvre
  - Accélération de l'implémentation logicielle des fonctions cryptographique dans le processeur RISC-V (open source 32-bit RISC-V ISA)
  - Chiffrement par bloc léger
- **Travaux en cours**
  - Protection du cryptoprocesseur contre les attaques par canal auxiliaire
- **Publications:** *IFIP ISTP2018 , IEEE ICECS2019, CryptArchi2019, IEEE DSD2020*

Utilisation de Ressources pour une Cible FPGA

Configuration	LWC instructions	LUTs	%	FFs	%
Basic ISA		937	-	765	-
Basic ISA+	SBOX	1355	+45	1822	+138
Basic ISA+	PRESENT_D	959	+2	766	+0.1
Basic ISA+	GIFT_D	976	+4	766	+0.1
Basic ISA+	PRINCE_D	1081	+15	768	+0.4
Basic ISA+	NMAT_D	1534	+64	1022	+34
PRESENT	SBOX+PRESENT_D	1368	+46	1823	+138
GIFT	SBOX+GIFT_D	1366	+46	1823	+138
PRINCE	SBOX+PRINCE_D	1494	+59	1825	+139
Midori	SBOX+NMAT_D	1979	+111	2079	+172
Twine	SBOX+NMAT_D	1979	+111	2079	+172
Skinny	SBOX+NMAT_D	1979	+111	2079	+172

Table: Consomation de Ressources des Instructions Supplémentaires



Gain en Vitesse d'Execution

Block Cipher	Base ISA	LWC ISA	Gain factor
PRESENT	12544	358	35
GIFT	10661	319	33
PRINCE	17357	126	138
Midori	18944	232	81
Twine	41279	622	66
Skinny	40887	409	100

Table: Nombre d'Instructions pour l'Execution de Différents Algorithmes

Architecture cryptographique adaptative

- **Problématique et approche**
  - Évolution des cas d'usage, des technologies, et des contraintes (CPU, mémoire, BP, ..)
  - Définition d'une suite d'algorithmes cryptographiques et d'un protocole flexible pour permettre la négociation d'algorithmes/paramètres à utiliser dans chaque cas
  - **Approche:** Combiner les notions de crypto-agilité et de cryptographie légère en offrant un compromis entre la sécurité de bout en bout et les performances
- **Doctorant :** Abdessamad Fazzat
- **Encadrants :** R. Khatoun & H. Labiod (TP), R. Dubois (Thales)
- **Travaux réalisés**
  - Analyse de performances des algorithmes cryptographiques utilisés pour sécuriser les communications internes et V2X
  - Conception d'un Crypto Manager (CM) permettant le choix adaptatif des algorithmes cryptographiques selon le contexte (attaque, QoS, update, etc.)
- **Travaux en cours**
  - Implémentation du CM, identification des scénarii de validation et analyse des performances
- **Publications:** CSNet2020, ICISSP2021

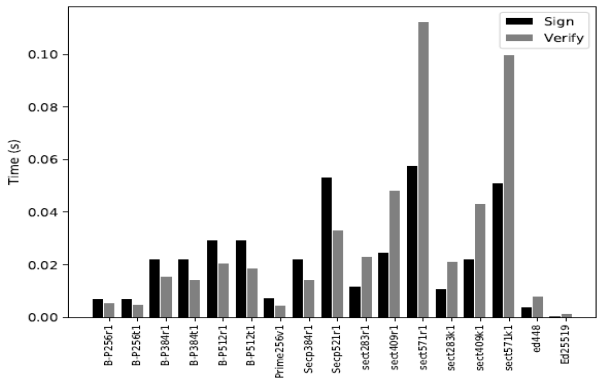


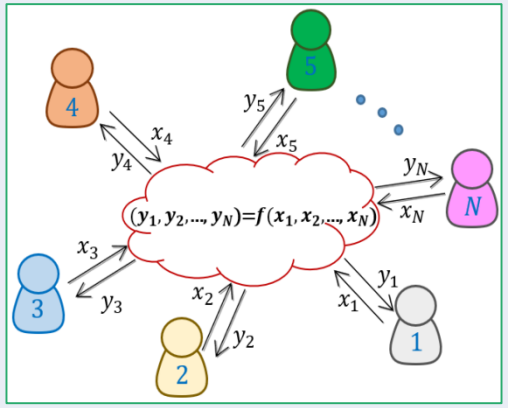
Figure: A comparison of elliptic curve digital signatures.

PERFORMANCE MEASURES OF NIST-ROUND2 AUTHENTICATED CIPHERS ON 2011 FREESCALE I.MX6 QUAD RUNNING AT 1200MHZ

Algo.	Block/Key	Encrypt (cycles/byte) 128	Encrypt (cycles/byte) 1536	Decrypt (cycles/byte) 128	Decrypt (cycles/byte) 1536
ACE	64/128	7153.59	4984.10	7193.42	4998.96
ASCON	64/128	101.11	83.45	103.40	26.19
COMET	128/128	154.66	109.89	157.85	110.51
DryGASCON	128/128	449.90	377.73	449.97	377.79
Elephant	64/128	39582.84	44254.79	39562.16	44267.12
ESTATE	128/128	9418.66	11520.51	9418.80	11513.72
ForkAE	128/128	2364.23	2870.05	3647.81	5451.68
GIFT-COFB	128/128	698.11	615.96	698.86	615.35
Gimli	128/128	146.12	99.98	147.45	101.73
Grain-128	128/128	208.73	180.62	210.16	182.55
HYENA	128/128	6350.23	5599.53	6350.41	5599.59
ISAP	64/128	18390.32	1381.48	18430.51	1378.83
KNOT	128/128	191.19	147.57	196.91	154.30
LOTUS	64/128	8719.23	10329.68	8719.50	10323.35
mixFeed	64/128	635.88	420.45	636.15	420.53
ORANGE	128/128	5082.32	4084.75	5084.12	4085.00
Oribatida	64/128	10769.70	10996.65	10777.18	10976.61
PHOTON	128/128	40678.51	39419.57	40671.10	39421.65
Pyjamask	128/128	1227.98	823.42	1221.02	809.38
Romulus	128/128	2936.19	3691.37	2944.53	3702.46
Saturnin	256/256	164.34	139.75	165.33	140.48
SKINNY	128/128	3060.85	4839.76	4116.26	2712.73
SPIX	128/128	3460.52	2004.86	3463.55	1999.21
SpoC	128/128	3372.17	2986.58	3371.49	3000.59
Spook	128/128	300.66	196.39	299.16	186.52
Subterranean	128/128	684.62	395.83	683.91	396.12
SUNDAE	128/128	1073.76	1214.31	1075.02	1215.65
TinyJambu	32/128	94.83	111.02	96.20	113.02
WAGE	128/128	1643.70	1152.96	1664.54	1151.79
Xoodyak	128/128	46.88	25.46	46.90	25.39

Un Postdoc

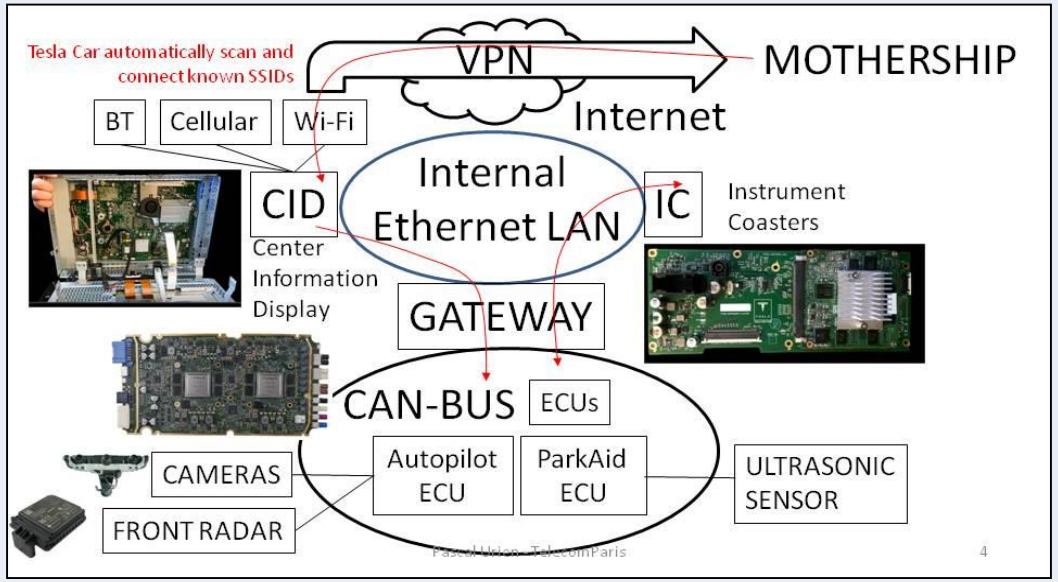
Partage et traitement distribué de données privées



- **Problématique & approche**
  - Manipulations des données privées en évitant toute fuite ou divulgation d'informations.
  - Deux cas d'usage
    - Sécurité des communications intra-véhicule et/ou avec l'extérieur
    - Partage et traitement anonyme de l'information en temps réel et de façon distribuée
  - **Approche :** Cryptographie distribuée
    - Créer des protocoles MPC (**multi-party computation)** sécurisés pour effectuer divers calculs sur des données privées et évaluer leurs performances vs. les mécanismes standardisés
- **Postdoctorant :** En cours de recrutement
- **Encadrants :** D. Hieu Phan, H. Labiod (TP), A. Dupin (Thalès)

Axe 3
Gestion des identités et authentification

- **Animateurs :** P. Urien (TP), D. Martinache (WS)
- **Problématique**
  - Nécessité d'authentifier les messages échangés au sein du véhicule (Échanges entre ECUs, paquets de diagnostic...)
  - Nécessité d'authentifier les messages échangés
  - Risque de vol de données personnelles
- **Approche**
  - Identity Framework (authentification, autorisation, sécurité des communications, données véhicule/utilisateur)
  - Résistance au hacking (attaques internes/externes)
- **Travaux en cours**
  - Chiffrement authentifié avec données supplémentaires (AEAD) appliqué au bus CAN
  - Procédure d'accès à la sécurité cryptographique
  - Sécurité de bout en bout pour la mise à jour du firmware



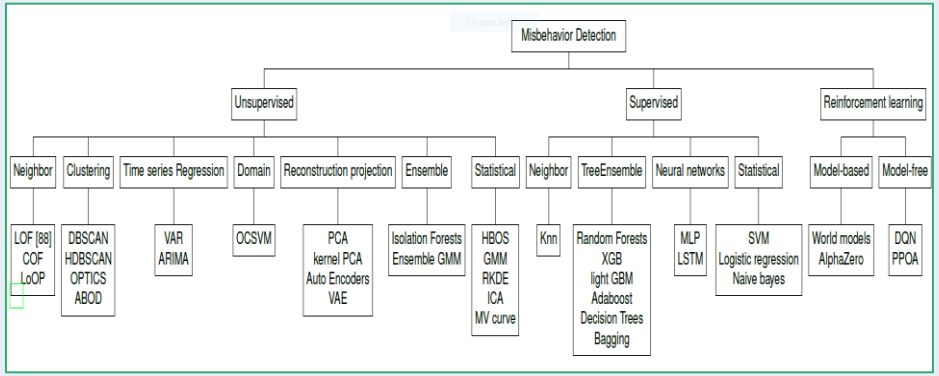
En recherche de candidat Postdoc
Modèle d'identité pour véhicule de nouvelle génération

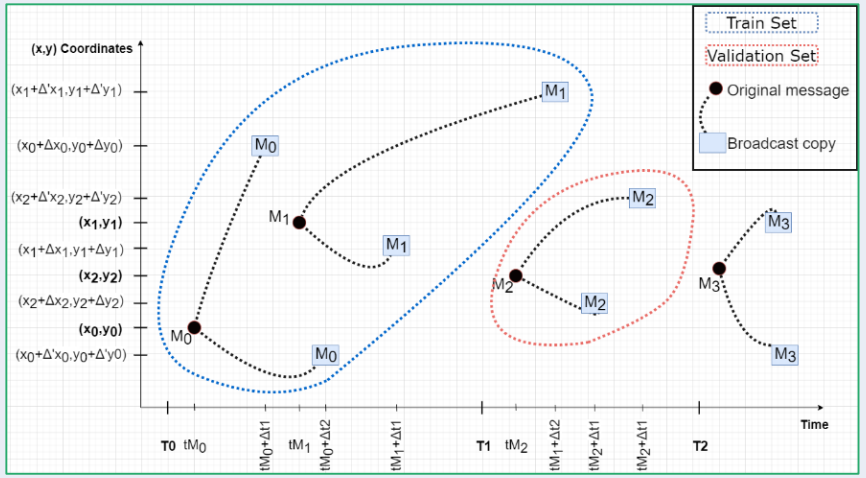
Axe 4
Résilience by design

- **Animateurs** : E. Borde, U. Kühne (TP), R. Moalla (Renault)
- **Problématique**
  - Nécessité de détecter des comportements anormaux provoqués par une cyberattaque inconnue
  - Nécessité de continuer à assurer des fonctions vitales liées à la conduite le temps de la mise en sécurité
- **Objectifs**
  - Mécanismes de détection de comportements anormaux distribués
  - Résilience : tolérance aux fautes (redondance), reconfiguration dynamique

Détection multi-niveaux de comportements anormaux

- **Problématique**
  - Les véhicules sont vulnérables aux cyberattaques et aux potentiels disfonctionnements.
  - Il est nécessaire de les détecter.
- **Doctorant :** Mohammed Lamine Bouchouia
- **Encadrants :** H. Labiod, O. Jelassi (TP), W. Benjaballah (TL)
- **Travaux réalisés**
  - Une nouvelle définition et classification des comportements anormaux
  - Une classification des méthodes Machine Learning utilisées pour la détection
  - Une nouvelle approche de subdivision des données pour l'entrainement des modèles machine learning dans le contexte du CAV permettant de résoudre le problème de fuites de données rendant le modèle plus performant dans la phase test/déploiement.
- **Travaux en cours**
  - Une architecture multi-niveaux pour la détection des comportements anormaux basée sur l'apprentissage par renforcement
- **Publications**
  - IEEE Communications Surveys & Tutorials 2021, SIAM2021





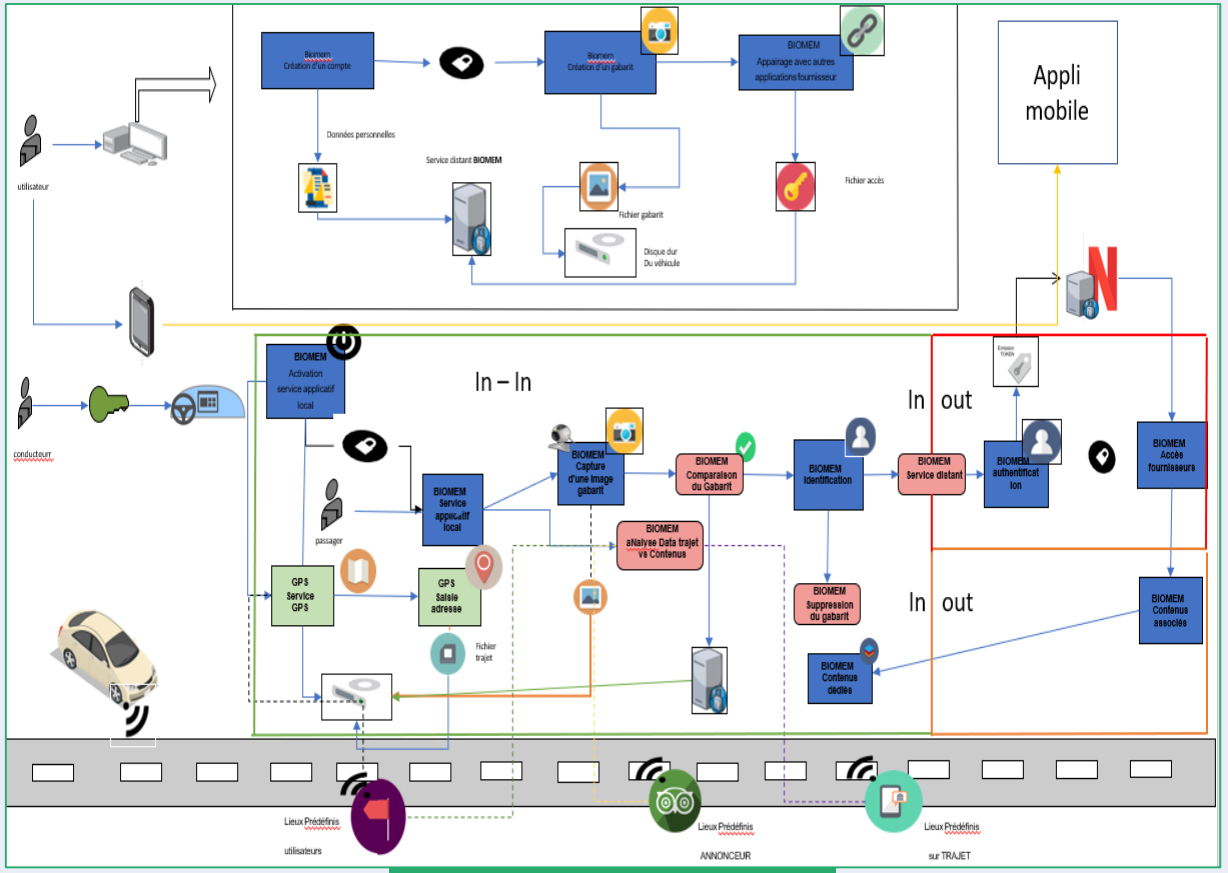
Deux autres thèses

- Adaptative architectural reconfiguration for improved resilience of connected cars
- **Problématique et approche**
  - Utilisation de techniques de reconfiguration dynamique et de *moving target defense* pour répondre à une attaque inconnue
- **Doctorant :** Maxime Ayrault
- **Encadrants :** E. Borde, U. Kühne (TP), B.Venelle (Valeo)
- **Publications :** ACM workshop on Moving Target Defense 2019

- Supervised Learning for Intrusion Detection Systems in Connected Cars
- **Problématique et approche**
  - Détection d'intrusion pour le véhicule connecté basée sur des mécanismes d'apprentissage supervisés
  - Complémentaire avec la thèse de Mohammed Lamine Bouchouia
- **Doctorante :** Natasha Alkhatib
- **Encadrants :** H. Ghauch, JL. Danger (TP), R. Moalla (Renault)

Axe 5
Confiance et données personnelles

- **Animateurs**
  - C. Levallois-Barth (TP), C. Jouvray (Valeo)
- **Contexte**
  - Flux de données personnelles au sein de l'écosystème
  - Risques liés à la création et à l'utilisation de ces données personnelles sur les plans sociétaux, techniques et juridiques
- **Objectifs**
  - Existe-t-il une méthodologie d'analyse d'impact relative à la protection des données personnelles (AIPD) adaptée à des traitements de données personnelles complexes, multipartites ?
    - dans un contexte de véhicules connectés
    - répondant aux critères posés par l'article 35 du Règlement Général pour la Protection des Données (RGPD)
- 1 Postdoc en Droit



Cas pratique (Biomem)

Collaboration chaire VP-IP / chaire C3S

Axe 5
Analyse d'impact relative à la protection des données personnelles

- **Problématique & approche**
  - Comment appréhender les risques ?
  - Analyse d'Impact sur les données personnelles, évaluation d'impact pour la Vie Privée, analyse d'impact éthique
- **Postdoctorant :** Jonathan Keller
- **Encadrants :** C. Levallois-Barth (TP), C. Jouvray (Valeo)
- **Travaux réalisés**
  - Tester 4 méthodologie d'analyse d'impact pour la protection des données personnelle CNIL, PRIAM, NIST, BSI
  - 3 types d'évaluation impact (AIPD, EIVP, EIA)
- **Travaux en cours**
  - Retours terrain d'experts tiers à C3S
    - Affiner la définition et la qualification du risque en matière de données personnelles
    - Repérer les points critiques des analyses d'impact
    - Renforcer l'aspect pratique du rapport final par une expertise métier
  - Rapport expertise juridique(120 pages), livre blanc
- **Publications :** Conférences(5), ateliers (5)