

Séminaire C4 2026

Clément Naves

Intelligent and secure sharing of sensitive data in the context of
connected vehicles

Done with the MUST project of the 5G PEPR



Contents

- 1 Topic presentation
- 2 Problem Generalisation
- 3 Main step
- 4 Secure Communication Channel creation
- 5 References

Topic presentation

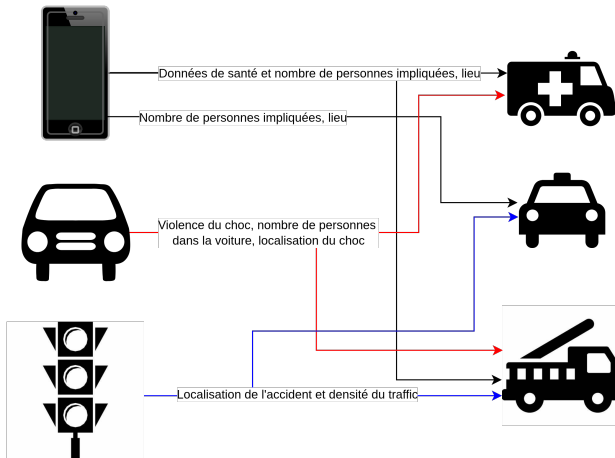


Figure 1 – Usecase

Problem Generalisation

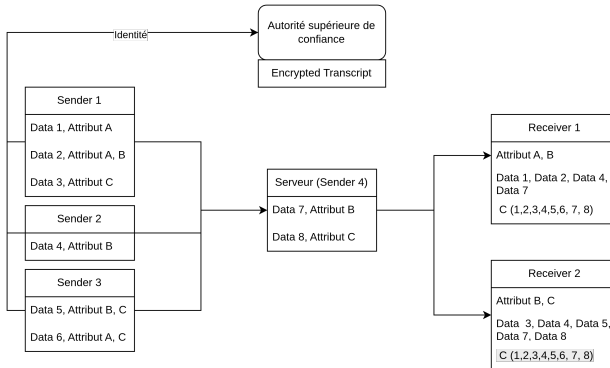


Figure 2 – Ideal data transfer

Problem Generalisation

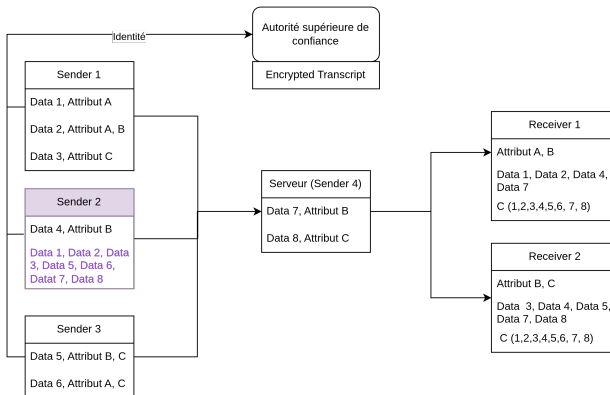


Figure 3 – Data transfer with malicious sender

Problem Generalisation

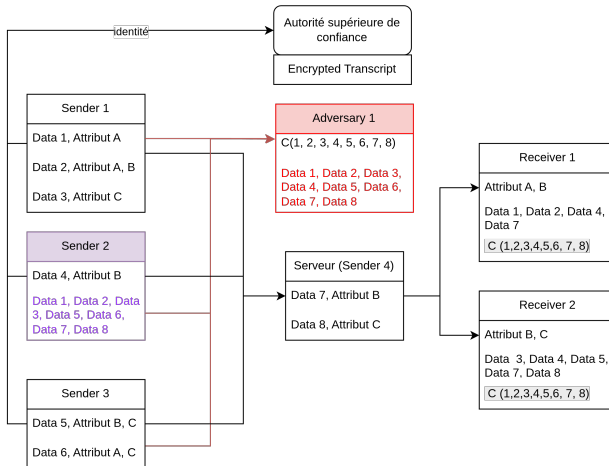


Figure 4 – Data transfer with sniffing adversary

Problem Generalisation

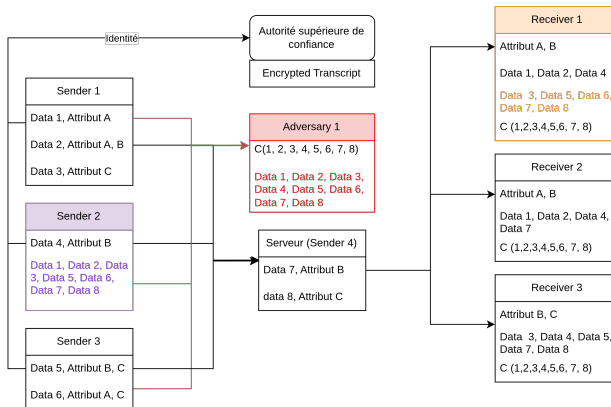


Figure 5 – Data transfer with malicious receiver

Problem Generalisation

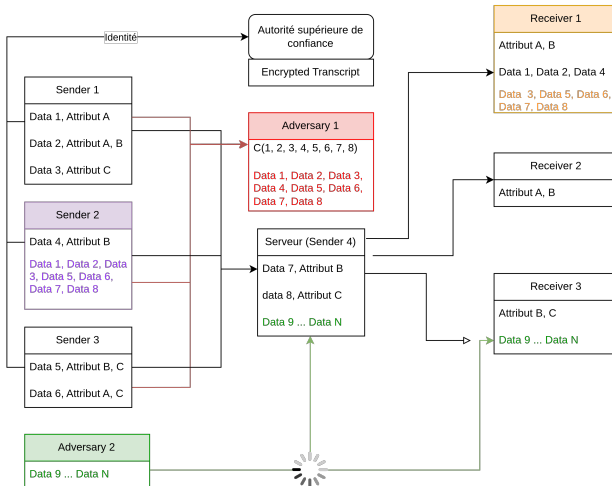


Figure 6 – Data transfer with corrupted data

Main step

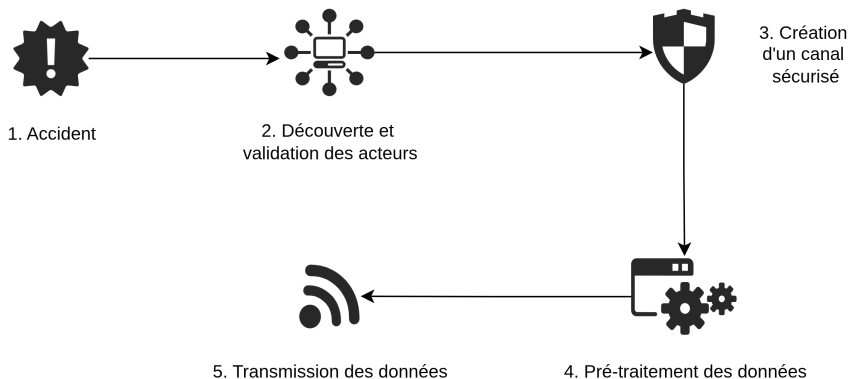


Figure 7 – Step of the protocol

Secure Communication Channel creation

- Indistinguishability
- Unforgeability (Unframability)
- Unlinkability (Anonymity)
- Parties can be part of many communication channels
- Exchange should be auditable and anonymity removed by a trusted Authority

References

- [NL26] Montassar NAGHMOUCHI et Maryline LAURENT.
Deanonymizable Scoped Linkable Ring Signatures.
arXiv :2605.11715 [cs.CR]. Mai 2026. DOI :
[10.48550/arXiv.2605.11715](https://doi.org/10.48550/arXiv.2605.11715). URL :
<http://arxiv.org/abs/2605.11715> (visité le
12/06/2026).
- [Per+22] Maharage Nisansala Sevandi PERERA et al. « A Survey
on Group Signatures and Ring Signatures : Traceability vs.
Anonymity ». en. In : *Cryptography* 6.1 (mars 2022), p. 3.
ISSN : 2410-387X. DOI :
[10.3390/cryptography6010003](https://doi.org/10.3390/cryptography6010003). URL :
<https://www.mdpi.com/2410-387X/6/1/3> (visité le
14/04/2026).

PERERA et al. (2022), « *A Survey on Group Signatures and Ring Signatures* » : survey sur les Ring et Group Signatures.

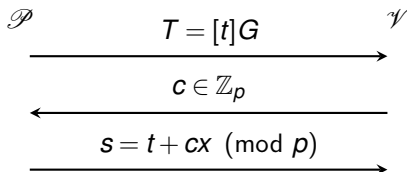
- Group signatures : anonymat dans un groupe, anonymat révocable.
- Ring signatures : facilité de la mise en place, anonymat irrévocable.

Schnorr ZKP over Elliptic Curves

Public parameters :

$$G \in E(\mathbb{F}_p)$$

The prover knows the secret $x \in \mathbb{Z}_p$ and publishes $X = [x]G$.



Verification

The verifier accepts if

$$[s]G \stackrel{?}{=} T + [c]X$$

Correctness

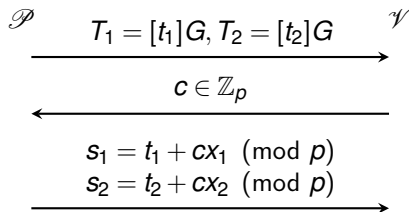
$$\begin{aligned} T + [c]X &= [t]G + [cx]G \\ &= [t + cx]G \\ &= [s]G \end{aligned}$$

Additive ZKP

Public parameters :

$$G \in E(\mathbb{F}_p)$$

The prover knows secrets x_1 and $x_2 \in \mathbb{Z}_p$ such that $X = [x_1 + x_2]G$ and publishes $X_1 = [x_1]G$, $X_2 = [x_2]G$, $X = [x_1 + x_2]G$.



Verification

The verifier accepts if

$$\begin{aligned} [s_1]G &\stackrel{?}{=} T_1 + [c]X_1 \\ [s_2]G &\stackrel{?}{=} T_2 + [c]X_2 \\ [s_1 + s_2]G &\stackrel{?}{=} T_1 + T_2 + [c]X \end{aligned}$$

Correctness

$$\begin{aligned} T_1 + T_2 + [c]X &= [t_1 + t_2]G + [c(x_1 + x_2)]G \\ &= [t_1 + cx_1 + t_2 + cx_2]G \\ &= [s_1 + s_2]G \end{aligned}$$

Non-Interactive Logical Or ZKP

Public parameters :

$$G \in E(\mathbb{F}_p)$$

The prover knows public X, Y and the secret x such that $X = [x]G$. It wants to prove that he knows whether x such that $X = [x]G$ whether y such that $Y = [y]G$.

$$\begin{aligned} t_x, s_y, c_y &\leftarrow \$\mathbb{F}_p^3 \\ T_y &= [s_y]G + [c_y]Y \\ c &= H(X, Y, T_x, T_y) \\ c_x &= c \oplus c_y \\ s_x &= t_x + c_x X \end{aligned}$$

Verification

The verifier receives c_x, c_y, s_x, s_y and accepts if

$$\begin{aligned} T_x &= [s_x]G - [c_x]X \\ T_y &= [s_y]G - [c_y]X \\ H(X, Y, T_x, T_y) &= c_x \oplus c_y \end{aligned}$$

For many elements

$$\begin{aligned} t_1 &\leftarrow \$\mathbb{F}_p \\ \{s_i\}_{i \in [2, n]} &\leftarrow \$\mathbb{F}_p^n \\ \text{for } i &\in [2, n] \\ c_i &= H(\{X_j\}_{j \in [1, n]}, T_{i-1}) \\ T_i &= [s_i]G + [c_i]X_i \\ c_1 &= H(\{X_j\}_{j \in [1, n]}, T_n) \\ s_1 &= t_1 + c_1 X_1 \end{aligned}$$

NAGHMOUCHI et LAURENT (2026), *Deanonymizable Scoped Linkable Ring Signatures*