Chair of Theoretical Information Technology
Department of Electrical and Computer Engineering
Technische Universität München

New Secure and Robust Protocols for 5G

Theoretical Information Technology – Prof. Dr.-Ing. Dr. rer. nat. Holger Boche

Biometric Authentication

Biometric data (or a Physical Unclonable Function) uniquely characterize a person (or device). This property qualifies them for being used in authentication. We consider the *two phase* biometric authentication process sketched in Fig. 1.

Enrollment Phase

- The authentication system receives the data X^n and the ID of a user.
- It generates helper message M and secret-key K.
- It uses one-way function f on K and stores the result and M in a public database under the user's ID.

Authentication Phase

- The authentication system receives the data Y^n and the ID of a user.
- It reads the helper message M and $f(K)$ from the database.
- It generates a secret-key $\hat{K}$.
- It compares $f(K)$ and $f(\hat{K})$.
- It accepts or rejects the user.

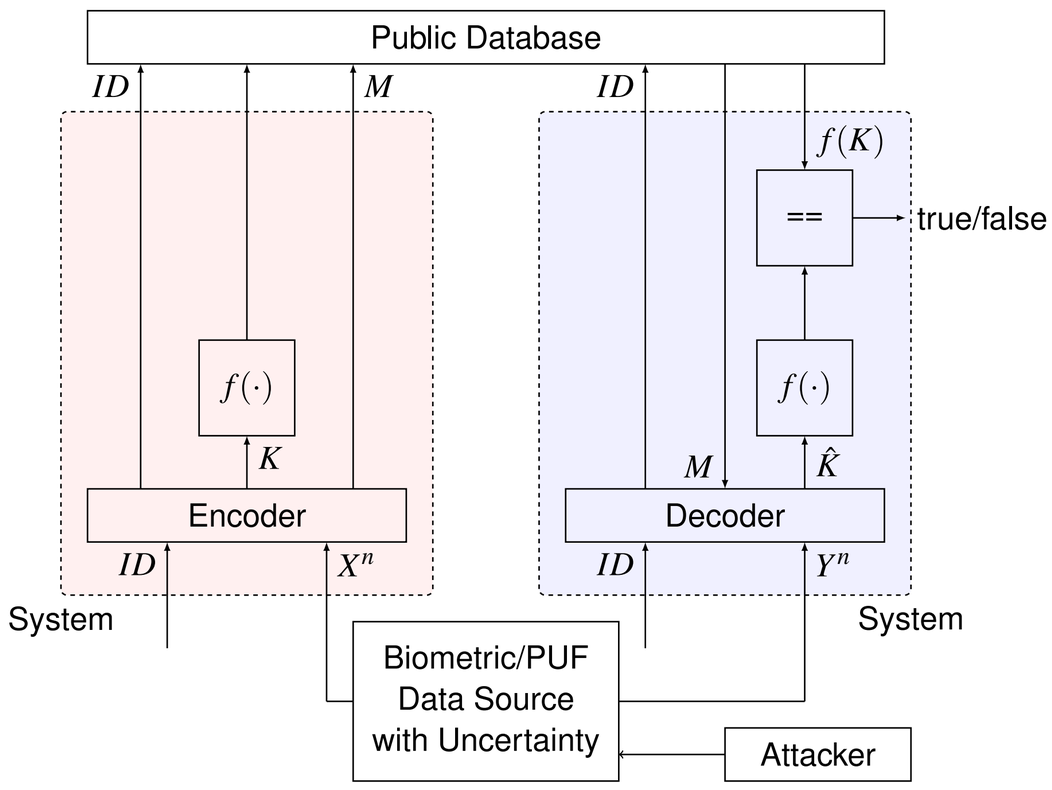

Fig. 1: Biometric authentication process with source uncertainty

Assumptions

- The source of the biometric/PUF data is not perfectly known.
- The attacker can influence the biometric/PUF data source.

Goals

- reliability: $\Pr(K=\hat{K}) \geq 1-\varepsilon$
- perfect secrecy: $I(M;K)=0$
- large key rate: $\frac{1}{n}\log|\mathscr{K}| \geq R-\varepsilon$
- uniformly distributed key: $H(K)=\log|\mathscr{K}|$
- control privacy leakage: $\frac{1}{n}I(X^n;M) \leq L+\varepsilon$

Result: Rate region

$$\mathscr{R}(\mathfrak{S}) = \bigcap_{\hat{s}\in\hat{\mathscr{S}}} \bigcup_{U_{\hat{s}}} \Big\{(R,L)\colon 0 \leq R \leq \min_{s\in\mathscr{I}(\hat{s})} I(U_{\hat{s}};Y_s)\ ,\ L \geq \max_{s\in\mathscr{I}(\hat{s})} I(U_{\hat{s}};X_s) - I(U_{\hat{s}};Y_s)\Big\}.$$

Robust and Safety-Related V2X-Communication

A major concern of 5G radio networks is a symbiosis of *robustness*, *low latency* and *high data rates* for information exchange. For this reason, the control information has to be managed in a reliable and low-latency manner while keeping the entertainment experience for secondary users unaltered. So next-generation networks have to be capable to adapt to different data traffic shapes. From a vehicular perspective, entertainment, infotainment as well as safety services are required to establish a safe, seamless and resilient user experience encompassing the connectivity between the driver, the vehicle and its surroundings. One very challenging use case is vehicle-to-X (V2X) communication for highly-automated driving or advanced driver assistance systems where large data packets (e.g., sensor data) have to be reliably transferred from the backend to the vehicle and vice versa with high speed.

Goals

- Ensure reliability of the communication link
- Robustness and security of the wireless V2X-link
- Enabling communication-assisted safety-related applications

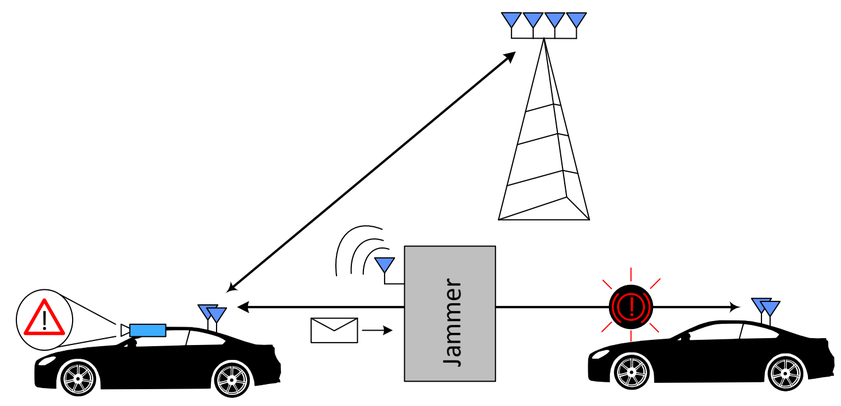

Fig. 2: AVC scenario in V2X-communication

Methods and First Results:

- Use information-theoretical methods to exploit structural properties of the communication channel $\Rightarrow$ avoid error events provoking system breakdown
- Control of the average and maximum error capacity by using diversity and specific coding mechanisms in scenarios with arbitrarily varying interference

$\Rightarrow$ Already $K=3$ antennas are sufficient to ensure the positivity of the capacity of the communication channel

$\Rightarrow$ Communication at positive rates for QPSK under state-constrained jamming

$\Rightarrow$ Important prerequisite: Antennas of the vehicular diversity antenna system have to be decoupled (due to spatial separation, pattern diversity, etc.)

Protocols for Secure and Robust Identification

Identification Approach [1]: In the theory of identification the goal of the Rx is changed compared to message transmissions in communication theory.

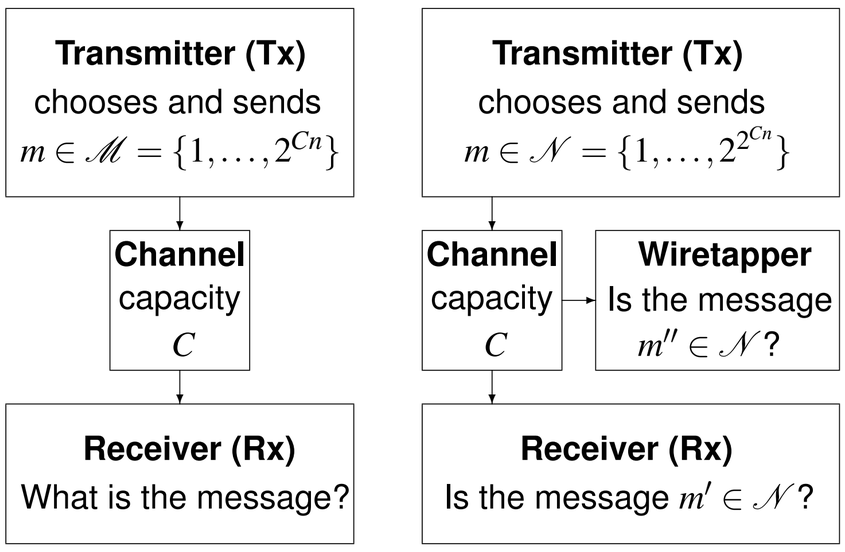

Fig. 3: Communication (left) and identification with a wiretapper (right)

Message Transmission

The Rx decodes the transmitted message. So the Rx must be able to decode all the messages from the Tx.

The number of codewords M_n of a transmission code has **exponential size** in the block length n of the codewords:

$$M_n = 2^{C\cdot n}$$

The **secure code** is always **smaller**.

Message Identification

The Rx has to decide if the message is equal to an arbitrarily selected message of the message set $\mathscr{N}$.

There are robust codes where the number of codewords has **double exponential size** in the block length n:

$$M_n = 2^{2^{C\cdot n}}$$

The **secure code** has the **same size**, if the secrecy capacity is positive.

Advantages of Identification based Communication Protocols

- Security and latency requirements can be embedded in physical transmission.
- Avoid limitations of message transmission in many applications.

Possible Applications: Communication solutions for Industry 4.0 and logistics applications, V2X and X2V Communication, Tactile internet [2]

[1] H. Boche and C. Deppe, *Robust and Secure Identification*, ISIT 2017.

[2] G. Fettweis, H. Boche, et al., *The Tactile Internet*, ITU-T Technology Watch Report, 2014.