講演番号	273

文献番号	20226273

Fault Attack and Its Software Countermeasure for In-Vehicle ECUs

Koji HORI[1)] Kohei KISHIMOTO[1)] Yuuki NAWA[1)]
Kyohei TAKEUCHI[1)] Kenichi KOGA[1)] Kazukuni KOBARA[2)]

1) TOKAI RIKA CO., LTD.
3-260 Toyota, Oguchi-cho, Niwa-gun, Aichi 480-0195, Japan
2) National Institute of Advanced Industrial Science and Technology (AIST),
Tokyo Waterfrontl, 2-3-26 Aomi, Koto-ku, Tokyo, 135-0064, Japan

KEY WORDS: electronics and control, microprocessor/large scale integrated circuit, electric circuit/electronic circuit, Fault Analysis, Voltage Glitch [E1]

Recently, vehicles communicating outside, so-called connected cars, are increasing. They exchange important data for vehicle control, such as the status of a vehicle and its surrounding states. In comparison with conventional vehicles, connected cars may be more seriously affected by cyber-attacks. Therefore, ensuring the security of ECUs, especially in connected cars, is crucial.

Even if connected cars adopt standardized cryptographic algorithms that have been evaluated carefully for a long time, attacks on the hardware might extract internal data such as cryptographic keys. One of the attacks on the hardware is called fault analyses, which triggers a malfunction in a device by injecting physical glitches from outside. Some cases of extracting internal data sets from the read-prohibited area have been reported, so they are real threats.

Attackers may have physical access easily to in-vehicle ECUs because vehicles are often parked outside. To clarify the risk, we examined whether or not the fault analysis is a realistic threat to in-vehicle ECUs. We performed a voltage glitch attack, one of the fault analyses, on an automotive-grade microcontroller. As a result, the microcontroller outputted a wrong value which might be used for cryptanalysis.

Then, we tested the effectiveness of a simple countermeasure that could be realized only with software. We implemented the countermeasure that performs the cryptographic processes multiple (n) times and then puts out the result only when the intermediate results match to avoid outputting a wrong value.

To bypass this countermeasure, the attacker must succeed in the malfunction injections multiple times in a row. The theoretical probability of the successful glitch on the microcontroller is about 0.0397^n, which is the n-th power of 3.97% (Fig.). We confirmed that for n=2 and got 0.16%, which is close to the theoretical probability of 0.0397^2. For n=3, it will be the cube. Therefore, it can reduce the success probability of the attack to an acceptable value depending on "n", the number of cryptographic operations.

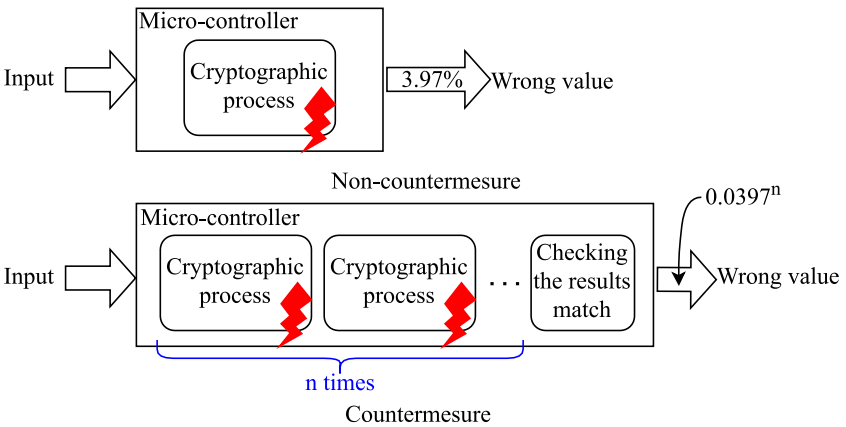

Fig. Countermeasure of the voltage glitch