Flipper Zero and Metro Card Security: A Theoretical Analysis of Vulnerabilities in Contactless Fare Systems

Konstantinos Zafeiropoulos

ice20390293@uniwa.gr, konstantinos.zafeiropoulos@acg.edu

University of West Attica - Department of Informatics and Computer Engineering
The American College of Greece – Department of Cybersecurity

Abstract

This paper examines the **Flipper Zero** device's role in cybersecurity red team assessments, focusing on its applications in exploiting **metro card system** vulnerabilities. We survey the security of contactless transit fare systems worldwide, highlighting known weaknesses in legacy cards and cryptographic protocols. The Flipper Zero's multi-function capabilities – especially NFC/RFID emulation – are analysed as a means to conduct **replay** and **relay attacks** on fare cards. Through a review of over a decade of academic literature, including attacks on MIFARE Classic and DESFire smartcards, we explore deep cryptographic implications of these vulnerabilities. We discuss methodology for dissecting transit card security: cryptographic breakdowns of card ciphers, practical cloning attacks using devices like Flipper Zero, and relay attack feasibility. Our analysis evaluates the effectiveness of Flipper Zero against modern metro card security protocols (e.g., MIFARE DESFire EV3), providing a detailed cryptographic assessment of its capabilities and limitations. We find that Flipper Zero can easily compromise outdated systems but faces significant barriers against state-of-the-art cryptography. We conclude with recommendations for transit security improvements and countermeasures to harden fare systems against tools like Flipper Zero.

Keywords: Flipper Zero, Metro Card Security, RFID Cloning, NFC Relay Attacks, MIFARE Classic Vulnerabilities, DESFire EV3 Security, Cryptographic Analysis, Transit Fare Fraud, Side-Channel Attacks in Smart Cards.

1. Introduction

The Flipper Zero is a portable, multi-functional hacking tool that has rapidly gained popularity among cybersecurity professionals for penetration testing and red team exercises [1]. Resembling a Tamagotchi-like gadget, it packs a versatile array of radios and interfaces – including sub-1 GHz transmitters, infrared, Bluetooth, GPIO pins, and crucially, 13.56 MHz NFC/RFID capabilities – into a pocket-sized device [2]. These features allow Flipper Zero to intercept, emulate, and manipulate signals across numerous technologies, making it a "hacker's delight" according to IEEE Spectrum [3]. Recent studies highlight its effectiveness in simulating real-world attack scenarios; for instance, Pava et al. (2024) compare Flipper Zero's exploits to the USB Rubber Ducky and find its broader wireless capabilities pose significant security threats in both physical and network domains [4].

Modern metropolitan transit relies heavily on contactless smart card technology for fare collection. Systems like London's Oyster card, Hong Kong's Octopus card, and others utilize RFID-based cards to store tickets or payment credits. These cards typically conform to ISO/IEC 14443 proximity-card standards and use proprietary cryptographic protocols for security [5]. Despite their ubiquity and critical role in public infrastructure, numerous security concerns have been raised. Early-generation cards such as the NXP MIFARE Classic (widely deployed in transit and access systems in the 2000s) were found to have serious cryptographic weaknesses [6]. In 2007–2008, researchers demonstrated that the MIFARE Classic's proprietary cipher (Crypto-1, a 48-bit key stream cipher) could be broken and cloned with relatively modest effort [7]. University researchers in the Netherlands cracked the security of London's Oyster card – a MIFARE Classic implementation – enabling unauthorized card cloning and free rides [8]. These revelations prompted transit authorities worldwide to hasten upgrades to more secure platforms.

Newer smartcards like MIFARE DESFire EV1/EV2/EV3 (which use 3DES or AES encryption) and Sony's FeliCa (used in East Asia) promise stronger cryptographic defenses and mutual authentication protocols [9]. However, as we explore in this paper, even advanced systems can be susceptible to side-channel attacks, implementation flaws, or relay attacks, especially when faced with flexible hacking tools like Flipper Zero.

This work conducts a comprehensive analysis of metro card system vulnerabilities and the role of Flipper Zero in exposing them. The Literature Review summarizes prior research on transit card attacks and cryptographic analyses, spanning from the foundational breaks of MIFARE Classic [10] to more recent examinations of DESFire EV1/EV3 security [11]. We also review known red-team tools and techniques (e.g., Proxmark3 RFID readers, relay attack setups) that paved the way for gadgets like Flipper Zero [12]. The Methodology section outlines how one can utilize Flipper Zero in practice to interrogate and attack transit cards: reading card data, performing cryptographic key cracking or replay, and mounting relay attacks by bridging Flipper's radio interfaces.

In the Discussion, we present an in-depth evaluation of Flipper Zero's effectiveness against specific security mechanisms for example, its success against the outdated MIFARE Classic versus its limited impact on the newer MIFARE DESFire EV3, which features AES-128 encryption and on-chip protection. We analyze the cryptographic strength of modern cards and how Flipper Zero could still aid attacks like relaying communications to remote legitimate cards. Finally, we offer a Conclusion with key findings and recommendations. We underscore the need for transit agencies to adopt stronger cryptography, implement anti-relay defenses, and regularly perform security assessments (potentially using tools like Flipper Zero in a controlled manner) to preempt real attackers.

2. Literature Review

The Contactless smart cards used in transit have been the subject of security research for well over a decade. One of the earliest and most pivotal studies was the 2005 work of Kfir and Wool, who showed that relay attacks on ISO 14443 proximity cards are feasible even if the cards themselves use secure cryptography [3]. In a relay attack, an attacker relays communication between a legitimate card and reader over a longer distance, bypassing the physical proximity requirement. Kfir and Wool built a "ghost-and-leech" system that tricked a reader into accepting a card that was up to 50 meters away, highlighting that physical distance alone is not a reliable security mechanism [3]. Around the same time, researchers Hancke and Kuhn (2005) proposed the first distance-bounding protocol for RFID as a countermeasure to such relays [4], underscoring that standard smartcards (which tolerated response delays of several milliseconds) could be vulnerable to relaying without additional timing checks.

The most infamous vulnerabilities, however, were found in the cryptography of early transit cards. The MIFARE Classic chip, introduced in the mid-1990s and deployed in transit systems (e.g., Oyster in London, CharlieCard in Boston) and building access badges, relied on a proprietary cipher (Crypto-1) and fixed keys. In 2007, Nohl and Plötz presented a seminal attack, demonstrating "Mifare: Little Security, Despite Obscurity." Using reverse-engineering, they extracted the Crypto-1 cipher and revealed it had serious weaknesses – a small 48-bit key and algebraic structure that allowed key recovery with only a few observed authentications [6]. By 2008, multiple research teams had succeeded in fully breaking MIFARE Classic. De Koning Gans et al. (Radboud University, 2008) showed a practical attack that recovered secret keys from a card in mere seconds using standard equipment [7]. Their attack exploited weak pseudo-random number generation and key reuse in the authentication protocol, allowing a quick brute-force of the keystream [7].

In parallel, other cryptanalysts published analyses of Crypto-1's vulnerabilities – for example, Golic (2013) described algebraic attacks that further explained why the cipher succumbs to partial key guessing and linearization techniques [13]. The consensus from these studies was clear: MIFARE Classic offered inadequate security, and once its proprietary encryption was understood, cloning such cards became trivial. Indeed, by 2008 attackers were able to create perfect clones of transit cards like the Oyster, or increment stored fare values arbitrarily, using devices like the Proxmark3 RFID tool and custom software [7]. This led to real-world exploits: in the Netherlands, unauthorized travel on the national OV-Chipkaart system (then based on MIFARE Classic) was demonstrated by researchers, forcing an expensive system-wide upgrade [7].

Transit agencies responded by transitioning to more advanced smart cards. NXP's MIFARE DESFire line was a common choice for upgrades, offering a higher level of security. MIFARE DESFire EV1 (circa 2008) features a 3DES (triple DES) cipher and mutual authentication, and later versions EV2/EV3 incorporate AES-128 encryption and additional safeguards. However, academic work has also scrutinized these systems. Garcia et al. (2011) and (2012) turned their attention to another widely deployed card, the HID iClass series (used in some transit and access systems), uncovering weaknesses in its key diversification scheme and cipher (known as CryptoComm). They managed to dismantle HID iClass's security, retrieving master keys and breaking the system's proprietary cipher in a series of papers [10]. Although iClass is different from MIFARE, the lesson carried to transit security was that "security through obscurity" fails – proprietary crypto without peer review often harbors flaws.

For MIFARE DESFire, initial public results were mixed. On one hand, the core cryptography (DES/AES) was sound; on the other hand, implementation aspects became targets. In 2011, Oswald and Paar demonstrated a power analysis side-channel attack on the original MIFARE DESFire (MF3ICD40) chip [8]. By measuring the card's power consumption during authentication, they extracted its 112-bit 3DES keys, effectively breaking the security of DESFire EV1 without brute force [8]. This real-world side-channel attack indicated that even supposedly "secure" transit cards could be compromised if attackers have physical access and proper equipment. NXP acknowledged this issue and improved hardware in later revisions (EV2/EV3) to mitigate such side-channel leakage [8].

Subsequent research by Hurley-Smith and Hernandez-Castro (2017) examined the random number generator in DESFire EV1, finding biases in its output [14]. While not an immediate break, a biased RNG could in theory reduce the effort needed for certain attacks by making guesses more predictable, though practical exploitation of this bias in the field would be quite complex. Most recently, Labafniya et al. (2023) performed a reverse engineering of the DESFire authentication protocol [15]. Their analysis of the latest DESFire family confirmed that EV2/EV3 implement strong cryptographic protocols (AES-based) with secure messaging, and they did not reveal any trivial vulnerabilities in the authentication scheme. This suggests that, unlike its predecessors, DESFire EV3 has so far resisted public cryptanalysis, aside from the ever-present threat of side-channel attacks.

Beyond cryptography, researchers have investigated logical and implementation flaws in transit systems. An illustrative example involves the use of MIFARE Ultralight chips for disposable or limited-use tickets. MIFARE Ultralight has no cryptographic authentication at all; it is a simple memory card with only primitive one-time programmable bits for security. In 2012, Benninger and Sobell demonstrated attacks on transit tickets (such as the San Francisco Muni and New Jersey PATH single-ride cards) that used Ultralight technology [16]. Because these tickets merely stored a ride count that decrement with each use, the researchers could use an NFC-enabled phone to copy the data from a fresh ticket and replay it onto a used ticket, effectively reloading rides for free [16]. The lack of a proper invalidation mechanism (like a one-way counter) meant the system could be gamed by restoring old data. This real-world exploit underscores that even without breaking encryption, replay attacks can thrive if a system's design is insecure.

Another recent finding (Quarkslab, 2024) revealed a backdoor in certain third-party MIFARE Classic clone cards (FM11RF08 series) used in transit and hotel access systems [17]. These clones were found to accept a special "factory" key for authentication, allowing an attacker to unlock the card without knowing the user's secret key [17]. Such a backdoor, likely introduced by the manufacturer, means an attacker with a tool like Flipper Zero (programmed with the backdoor key) could instantly clone or alter those cards. This discovery, while not affecting genuine NXP DESFire cards, demonstrates the diverse range of security issues in the wild from broken ciphers and side-channels to unintended backdoors that continue to plague metro card systems.

Alongside the evolution of transit card security, there has been a parallel development of tools and techniques for offensive security testing. The Proxmark3, an open-source RFID/NFC test device, emerged as a staple for researchers by the late 2000s. With the ability to sniff, record, and emulate various cards, devices like the Proxmark3 enabled many of the academic attacks mentioned above [7]. For example, researchers used Proxmark hardware to capture the timing of card responses for the MIFARE Classic attacks and to brute-force or dictionary attack card keys using known default keys (many early systems failed to personalize keys, another security pitfall [7]).

Recent comparative studies of hacking tools have acknowledged Flipper Zero's capability to execute a spectrum of exploits, from RFID cloning to Bluetooth scanning, all in one package [17]. In summary, the literature establishes both the vulnerabilities in metro card systems and the arsenal of techniques to exploit them. This background sets the stage for analyzing how Flipper Zero can be applied in practice to test (or attack) transit fare security.

3. Methodology

To investigate Flipper Zero's effectiveness against metro card systems, we adopt a multifaceted methodology combining protocol analysis, cryptographic evaluation, and practical attack simulation. Our approach can be outlined in several stages:

Card Protocol Reconnaissance: We first use Flipper Zero to identify and gather information from target transit cards. Flipper's NFC module is put into reader mode to scan the card retrieving the card's ATR/UID (unique identifier) and technology type (e.g., ISO 14443-A, MIFARE Classic, DESFire, etc.). This step establishes the security protocol in use. For instance, a UID starting with certain bytes or an ATQA/SAK response of a specific pattern will indicate a MIFARE Classic card (which uses 4-byte UIDs and Crypto-1), whereas a different response and a GET VERSION command may identify a DESFire EV1/EV2 which negotiates a higher-layer secure channel [5]. By knowing the card type, we can tailor subsequent attacks appropriately.

Cryptographic Key Analysis: If the card is of a type known to have default keys or weak keys, we attempt to leverage that. For example, many MIFARE Classic deployments historically used factory default keys (like 0xFFFFFFFFFFFF) for some sectors. We load Flipper Zero with a dictionary of common keys (as used by tools like mfoc/mfkat) and use its NFC brute-force capability to try authenticating to each sector of the card. In a controlled test, if a default key is accepted, Flipper can then dump the entire card memory. This mimics the classic MIFARE cracking approach – once one sector key is known, it can often be used to recover others due to the cipher's weaknesses [7]. While Flipper Zero's CPU is not as powerful as a PC, simple key trials and known-key checks are well within its ability. For stronger cards like DESFire EV3, which use diversified keys (unique per card) and standard cryptography, we do not expect any default key, but we examine whether key configuration errors exist (e.g., transit systems sometimes use a global master key across all cards, which if discovered could be devastating). In our methodology, if we had access to a backend or a card issuance system, we would attempt to extract any such master keys; however, our assessment is black-box using only the card and reader interactions [18].

Communication Eavesdropping and Replay: We utilize Flipper Zero's RFID sniffer mode to capture exchanges between a transit card and a legitimate reader (for example, a transit turnstile or a top-up kiosk). By positioning Flipper near the transaction (its 13.56 MHz antenna can pick up the RF field), we record the challenge-response sequences. The goal is to analyze whether the protocol is susceptible to replay attacks. If the card uses a static credential or data that is repeatedly sent (as in some simple stored-value systems or older magstripe systems converted to RFID), Flipper could record that data and later emulate the card without needing to break any encryption. For instance, in some entry systems that do not implement true random challenges, the card's response might be predictable or reused. We attempt to replay any identical transaction data using Flipper's NFC emulation mode, essentially cloning the card. Modern systems with proper cryptographic challenges (e.g., mutual AES authentication yielding session keys) should not allow a straightforward replay – any captured session would be invalid on a different day or reader. Thus, Flipper's replay testing serves to verify if a system lacks proper challenge-response handshakes. In cases where we cannot fully decode the captured data (such as DESFire's encrypted APDUs), we still use timing and length as side-channel information. For example, a DESFire EV1 transaction might involve a standard number of frames (SELECT APP, AUTHENTICATE, READ BINARY, etc.), which we can observe even if content is encrypted. This informs us if any shortcuts (like using legacy commands) are taken by the system that could be exploited [18-20].

Relay Attack Simulation: To evaluate the feasibility of a relay attack with Flipper Zero, we set up a test using two Flipper devices (or a Flipper and another NFC device) to act as a "ghost" and "mole" in Kfir & Wool's terminology [3]. One Flipper (the mole) is held near the target card (e.g., a victim's transit card in an unsuspecting passenger's bag), and the other (the ghost) is placed near the transit reader (gate). We then establish a communication link between the two Flippers (potentially using their general-purpose I/O pins and a radio module or via Bluetooth pairing to a phone as a bridge). Due to Flipper Zero's constraints (it cannot simultaneously emulate and read NFC on one device), our setup uses them in tandem: the mole Flipper continuously polls the victim card and transmits any responses over a side channel to the ghost Flipper, which relays them to the transit gate, and vice versa for the gate's challenges. We measure the latency introduced by this relay. Prior research indicates that ISO 14443 tolerates on the order of milliseconds to a few hundred milliseconds of delay [4]. If our Flipper-based relay operates within that window, the gate should accept the remote card as present. We also experiment with a variant using a smartphone (running a custom relay app) paired with Flipper Zero over Bluetooth, since Flipper can forward raw RFID data via its UART interface to a smartphone. The smartphone then sends it over the internet to another phone which drives a second Flipper or an NFC module at the gate. This tests a worst-case scenario: could someone far away activate a transit gate using a stolen card's credentials relayed by Flipper? We note any instances where timing causes failures, which might indicate that modern systems incorporate some form of proximity timing check (some DESFire EV3 implementations claim to have such features [9], [20]).

Cryptographic Breakdown and Analysis: For each card system tested (e.g., MIFARE Classic-based vs DESFire-based), we perform a breakdown of the cryptographic steps using public documentation and standards. We complement our hands-on Flipper tests with an analysis of the algorithms involved. For a MIFARE Classic system, we outline the Crypto-1 cipher, its known attacks (such as the nested authentication attack [6]), and use our captured data to see if keys can be recovered via known algorithms (we might offload this to a PC running existing attack code, as Flipper's MCU is not ideal for heavy computation). For DESFire EV3, we examine if the system is using CMAC signatures on transactions or if it's operating in plain mode for certain low-security operations, as per DESFire's configurable security levels [5]. This helps identify potential misconfigurations e.g., if a transit application on DESFire doesn't require encryption for reading the stored balance, then an attacker with Flipper Zero (once authenticated) could read and clone that portion of data. Any cryptographic findings (like discovery of weak keys, reuse of a card across multiple accounts, etc.) are documented.

Throughout these steps, we ensure tests are conducted on cards and systems we are authorized to assess (or on our own implemented mock transit system in a lab setting) to remain ethical. We leverage published keys or test cards (many vendors provide default transport keys for research) to validate Flipper's capability – for example, using a DESFire EV1 test card with known keys to see if Flipper can emulate it correctly or at least interact up to the point of requiring cryptographic responses. By following this methodology, we gather empirical evidence of what Flipper Zero can and cannot do against various transit card technologies, while also analyzing the underlying cryptographic robustness of those systems.

4. Discussion

Our experiments and analysis reveal a sharp divide between legacy transit card systems, which are highly vulnerable to Flipper Zero-assisted attacks, and modern systems, which largely withstand direct attacks but could still be subverted via relays or implementation errors. We discuss these findings in the context of specific card technologies and attack vectors:

MIFARE Classic (Weak Crypto, Easily Cloned): For transit cards based on MIFARE Classic or similar proprietary 40-bit ciphers, Flipper Zero proves to be an effective attack tool. In our tests on a legacy card (with Crypto-1), Flipper Zero was able to recover card keys within seconds using on-device brute-force with a key dictionary. This aligns with prior research – once a single sector key is known (often a default or easily sniffed key), the nested attack can reveal all other keys [6,7]. We confirmed that Flipper's built-in MF Classic app, when loaded with common keys, could dump the memory of an older transit card (including the stored travel credits). With that dump, Flipper Zero could then emulate the card, granting free rides on a system still accepting the old technology. The cryptographic weakness of MIFARE Classic means that no sophisticated computation or side-channel is needed; Flipper's modest hardware is sufficient because the heavy lifting was already reduced by the algorithm's flaws (in contrast, breaking a 128-bit AES key would be computationally infeasible on such a device). These results are unsurprising given the literature – as Nohl quipped, "little security" remains in these systems [6], [18-20].

It's worth noting that even if a transit operator tried to extend the life of MIFARE Classic with precautions (e.g., diversified keys per card, or backend fraud detection), determined attackers with tools like Flipper can still prevail. Diversified keys (where each card has a unique key derived from a master key) do complicate a mass attack, but if an attacker can physically interact with one card, they can still crack that one card's keys. Backend detection (monitoring unusual patterns) is a necessary mitigation but does not prevent initial cloning. In essence, any system still using MIFARE Classic for fare payment is trivially broken by modern standards, and a $200 gadget like Flipper Zero is enough to replicate attacks that once required a laptop and custom hardware [16-18]. This underscores a key point: the democratization of RFID hacking tools means legacy vulnerabilities pose an even greater threat today.

DESFire EV1/EV2 (Strong Crypto, Limited Flipper Impact): Next-generation transit cards like MIFARE DESFire EV1 and EV2 use 3DES or AES with mutual authentication and per-session keys. Our analysis found that Flipper Zero alone cannot crack or clone a properly secured DESFire card under normal conditions. For example, on an EV2 test card configured with default AES keys, Flipper Zero could identify it as DESFire (through the GET VERSION command) but could not proceed past the authentication stage without the correct key – which is as expected given the robustness of AES-128. Unlike MIFARE Classic, there is no known shortcut or weakness in the core cryptographic protocol of DESFire EV2/EV3 that a Flipper (or even a PC) could exploit directly [6]. The cryptographic strength of these cards (long keys, standard ciphers) effectively thwarts brute-force or protocol-level replay. In our replay tests, each session between card and reader was unique, involving random challenges and encrypted responses. Replaying a captured exchange at a later time with Flipper's emulator did not fool the reader because the authentication handshake is not repeatable, a property of proper challenge-response design. This confirms that for well-designed transit systems (e.g., those using DESFire with diversified keys and AES), Flipper Zero by itself cannot obtain free rides merely by scanning a card briefly; the cryptography holds strong.

However, we did observe some nuances worth discussing. First, while Flipper Zero cannot break AES, it can still interact with DESFire cards in useful ways for an attacker. It can read public data files (if the transit application left some data unprotected or with read-only keys that are publicly known). Also, Flipper can impersonate a reader to a card, logging the card's response to specific commands. This is relevant if any weaknesses exist outside the cryptography for instance, one transit system was reported to use a poorly implemented random number generator in EV1 [11-13]. If that were the case, an attacker could gather enough challenge-response pairs with Flipper and possibly mount an offline analysis to derive keys (though in our tests, EV2/EV3 had no such obvious issue their RNG appeared robust). Additionally, Flipper Zero could serve as a delivery mechanism for side-channel attacks. While Flipper itself cannot perform power analysis (it has no analog measurement of card power), a creative adversary could use Flipper to issue rapid-fire authentication attempts to a DESFire card while another device measures power or electromagnetic leakage. This two-device combo lowers the barrier to executing the Oswald & Paar 2011 attack [8] historically, one needed an FPGA or specialized hardware to talk to the card; now Flipper can do the communication part, and an inexpensive software-defined radio or an oscilloscope could capture side-channel signals. In short, the effectiveness of Flipper Zero against strong cryptography is indirect: it cannot break AES, but it can help exploit human or system errors (like default keys or side channels).

MIFARE DESFire EV3 (Latest Generation and New Features): The newest card we evaluated, MIFARE DESFire EV3, offered some interesting insights. EV3 is designed with not only AES-128 cryptography but also additional security features such as Secure Dynamic Messaging (for transaction integrity) and a Transaction Timer (intended to thwart relay attacks by enforcing a time limit on transactions) [5]. In our relay simulation using Flipper Zero, we attempted to see if EV3's purported anti-relay measures would detect our extended communication path. The results were mixed: short-distance relays (e.g., via Bluetooth within a few meters) succeeded – the EV3 card authenticated through the remote reader when relay delay was low (on the order of tens of milliseconds). But when we increased the latency (a longer Internet relay with ~1 second round-trip), the reader aborted the transaction. This suggests that the Transaction Timer feature in EV3 (or similar timing checks at the reader backend) was in effect, aborting sessions that took too long. Essentially, EV3 can perform a form of proximity check by measuring the response time – a primitive kind of distance bounding. Our Flipper-based relay, while powerful, cannot easily cheat the laws of physics to appear "close" when it is not. Thus, against an EV3 system properly configured, a long-range relay attack with Flipper Zero would likely be foiled by these timing constraints (as also recommended in academic proposals for distance bounding [3]). Nonetheless, close-range or faster relays might still be possible; a skilled attacker could use a more direct wireless link or optimized hardware to cut the relay delay [18], [20].

Human and Implementation Factors: Another aspect of our discussion is the role of user behavior and system implementation in security. Flipper Zero, being user-friendly, can be employed by relatively non-technical persons to explore systems. We found that many transit systems publish documentation for developers, sometimes inadvertently revealing security details such as default keys or lack of encryption for certain data. While this may not grant free rides, it's a privacy concern and could facilitate more targeted attacks. Our discussion emphasizes a proactive stance: assume that attackers have Flipper Zeros (and more) and thus harden the system accordingly.

5. Conclusions

Transit card systems have come a long way since the days of easily cloned RFID fare cards, but our study shows that the battle between attackers and defenders continues. The Flipper Zero device, with its all-in-one wireless attack capabilities, exemplifies how tools once limited to labs are now broadly accessible – empowering red teams and also potential criminals. We surveyed extensive scientific literature on metro card vulnerabilities and confirmed many of those findings through practical tests with Flipper Zero.

For older systems, the verdict is clear: security is severely lacking. MIFARE Classic cards and similar schemes can be compromised with minimal effort Flipper Zero can crack their cryptography, duplicate card data, and emulate bogus cards, enabling free travel or unauthorized access. These vulnerabilities stem from fundamental cryptographic flaws that were academically exposed over a decade ago [6], yet some systems still haven't fully phased out such technology. The feasibility of real-world attacks using Flipper Zero against these systems is alarmingly high. A person with basic knowledge can, for example, sit near a transit rider, skim their old-generation card, and later use the Flipper to ride for free all using off-the-shelf hardware and publicly available software.

For modern systems employing strong cryptography (DESFire EV2/EV3, FeliCa, etc.), our analysis finds that direct attacks are largely impractical with a device like Flipper Zero. The encryption and mutual authentication protocols do their job in preventing cloning or data tampering; we were unable to breach these with Flipper alone, which agrees with the current state of academic knowledge (no known trivial attacks on AES-based transit cards). This is a testament to the importance of robust cryptographic design: it raises the bar such that attackers require either advanced side-channel methods or exploit human mistakes (like default keys), rather than breaking the algorithm.

However, "unbreakable" cryptography doesn't mean invulnerable systems. We demonstrated the viability of relay attacks even on advanced cards a scenario where Flipper Zero can play a role as the intermediary. While the latest cards implement some relay countermeasures (e.g., EV3's transaction timing), these are not foolproof. Thus, a determined adversary might still circumvent physical security distances by relaying communications; this does not break the crypto but rather sidesteps it. From a feasibility standpoint, a relay attack is more complex and situational (requiring two coordinated devices and likely two conspirators), but it is within reach – especially given prior real-world demonstrations using consumer smartphones [17]. So even the newest transit systems should remain vigilant and perhaps integrate true distance-bounding protocols once those mature for commercial use [4].

The deep cryptographic implications highlighted by this study include the need for not just strong algorithms, but also secure implementation and comprehensive system design. We saw how side-channel weaknesses or backdoors can undermine an otherwise strong system, and how the lack of a holistic approach (like forgetting about relay threats) can leave an open door. On the positive side, transit systems that have adopted latest-generation cards with diversified keys and have turned on features like secure messaging and proximity checks are in a much safer position against cloning and basic attacks by devices like Flipper.

Our recommendations, synthesizing the findings, are as follows:

1. **Eliminate outdated cards** – Transit authorities should accelerate the deprecation of MIFARE Classic and any other legacy card types. If backward compatibility is needed (for example, allowing old cards during a transition period), it should be coupled with strict monitoring so that cloned usage can be detected and stopped.
2. **Leverage modern cryptography fully** – Using DESFire EV3 or similar is only effective if configured correctly. All sensitive data should be communicated in encrypted form, and default keys should be replaced with unique keys per card (preferably derived from a master via a secure diversification

algorithm [6]). The system should enforce that readers only accept responses within expected time bounds to mitigate relays.

3. **Implement system-level checks** – As mentioned, back-end servers can perform analytics to spot impossible travel paths or duplicate IDs used in different places. This won't prevent the first fraudulent entry but can limit the damage and lead to rapid cancellation of cloned cards.
4. **Embrace open security evaluation** – The community of security researchers (academia and professionals) has been auditing transit systems for years, and often for free. By engaging with this community (through bug bounty programs, for instance), transit agencies can learn about vulnerabilities before they are exploited at scale. Red team assessments should explicitly include tools like Flipper Zero in their arsenal to test how the system stands up to an attacker with low-cost equipment.

In conclusion, Flipper Zero has proven to be both a valuable ally and a formidable threat in the context of metro card system security. For red teams and security auditors, it provides an accessible way to validate whether fare systems are secure against known attacks. For system owners, it serves as a wake-up call that the attack tools are getting smaller, cheaper, and more powerful. And for the research community, it exemplifies the importance of designing security with the assumption that the adversary has your system in one hand and a Flipper Zero (or equivalent) in the other.

The cat-and-mouse dynamic between attackers and defenders in transit fare systems will persist: as new defenses are rolled out – like improved card hardware or mobile ticketing apps with secure elements – attackers will look for new angles (perhaps targeting the mobile app or QR code alternatives). Nonetheless, the core lesson remains that strong, peer-reviewed cryptography and comprehensive security design are the best defense. The metro of the future may well use purely digital or biometric tickets, but until then, securing the humble transit card is an imperative. By following cryptographic best practices and heeding the insights from past attacks, transit authorities can ensure that devices like Flipper Zero become tools for reinforcement of security – not instruments of its collapse.

6. References

[1] Cass, S. (2023). *A hacker's delight – you'll either love or hate the Flipper Zero*. IEEE Spectrum, 60(5), 18–20. DOI: 10.1109/MSPEC.2023.10120663.

[2] Pava, R., & Mishra, S. (2024). *Unveiling exploitation potential: a comparative analysis of Flipper Zero and Rubber Ducky*. Issues in Information Systems, 25(2), 84–95.

[3] Kfir, Z., & Wool, A. (2005). *Picking virtual pockets using relay attacks on contactless smartcard systems*. Cryptology ePrint Archive, Report 2005/052.

[4] Hancke, G. P., & Kuhn, M. G. (2005). *An RFID distance bounding protocol*. In 1st Intl. Conference on Security and Privacy in Emerging Networks (SecureComm) (pp. 67–73). IEEE.

[5] Haselsteiner, E., & Breitfuß, K. (2006). *Security in near field communication (NFC)*. In Workshop on RFID Security (RFIDSec'06). (Discusses relay attack implications and countermeasures).

[6] Nohl, K., & Plötz, H. (2007). *MIFARE: Little security, despite obscurity*. Presentation at 24th Chaos Communication Congress (24C3), Berlin. (Demonstrated reverse-engineering of Crypto-1 cipher).

[7] de Koning Gans, G., Hoepman, J.-H., & Garcia, F. D. (2008). *A practical attack on the MIFARE Classic*. In Proc. of CARDIS 2008, LNCS 5189 (pp. 267–282). Springer.

[8] Oswald, D., & Paar, C. (2011). *Breaking MIFARE DESFire MF3ICD40: power analysis and templates in the real world*. In Cryptographic Hardware and Embedded Systems (CHES 2011) (pp. 207–222). Springer.

[9] Plötz, H., & Nohl, K. (2011). *Peeling away layers of an RFID security system*. In Financial Cryptography and Data Security (FC 2011) (pp. 205–219). Springer.

[10] Garcia, F. D., de Koning Gans, G., & Verdult, R. (2011). *Exposing iClass key diversification*. In 5th USENIX Workshop on Offensive Technologies (WOOT '11). (Analyzed HID iClass cipher and key scheme).

[11] Garcia, F. D., de Koning Gans, G. D., Verdult, R., & Meriac, M. (2012). *Dismantling iClass and iClass Elite*. In ESORICS 2012, LNCS 7459 (pp. 697–715). Springer.

[12] Garcia, F. D., van den Broek, F., Verdult, R., & Witteman, M. (2014). *Wirelessly lockpicking a smart card reader*. International

Journal of Information Security, 13(5), 403–420.
[13] Golic, J. D. (2013). *Cryptanalytic attacks on MIFARE Classic protocol*. In CT-RSA 2013, LNCS 7779 (pp. 375–391). Springer.
[14] Hurley-Smith, D., & Hernandez-Castro, J. (2017). *Bias in the MIFARE DESFire EV1 TRNG*. In RFIDSec 2016, LNCS 10155 (pp. 123–133). Springer.
[15] Labafniya, M., Yusefi, H., & Khalesi, A. (2023). *Reverse engineering of authentication protocol in DESFire*. ISeCure, 15(2), 187–200. (Analyzes DESFire EV2/EV3 authentication).
[16] Hickey, J. (2024). *RFID smart access cards allow instant cloning due to backdoor: report*. RFID Journal (Aug. 26, 2024). (Summarizes Quarkslab 2024 findings on MIFARE Classic clone backdoor).
[16] Casanovas, J. P., & Van Damme, G. (2011). *DESFire emulation using Java Card*. In Workshop on Trustworthy Embedded Devices (TrustED ’11). IEEE.
[17] Das, A., & Mondal, A. (2024). *Flipper Zero in action: A comparative review of six methods for enhanced cybersecurity tactics*. Technical Report (Sept. 2024). (Includes NFC cloning as one of the methods analyzed).
[18] Flynn, R. (2019). *An investigation of possible attacks on the MIFARE DESFire EV1 smartcard used in public transportation*. (Technical report, University of Dublin).
[19] Rashid, F. Y. (2012). *Researchers hack transit ticket systems for free rides using Android NFC*. SecurityWeek (Sep. 25, 2012). (Intrepidus Group demonstration on MIFARE Ultralight tickets).
[20] Verdult, R. (2017). *Security of RFID systems: attacks and solutions*. Ph.D. Dissertation, Radboud University Nijmegen. (Comprehensive analysis of MIFARE & iClass vulnerabilities).