An automobile security protocol: side-channel security against timing and relay attacks

Article *in* International Journal of Electronic Security and Digital Forensics · July 2017

DOI: 10.1504/IJESDF.2017.10005632

5 authors, including:

Norhaflyza Marbukhari
Universiti Teknologi MARA
4 PUBLICATIONS **1** CITATION
SEE PROFILE

N.N. Mohamed
Mahsa University College
19 PUBLICATIONS **44** CITATIONS
SEE PROFILE

Mohd Anuar Mat Isa
Malaysian Institute of Microelectronic Systems
47 PUBLICATIONS **150** CITATIONS
SEE PROFILE

Syed Farid Syed Adnan
Universiti Teknologi MARA
27 PUBLICATIONS **104** CITATIONS
SEE PROFILE

An Automobile Security Protocol: Side-channel Security against Timing and Relay Attacks

Mohd Anuar Mat Isa [1]

Habibah Hashim [2]

Syed Farid Syed Adnan [3]

Norhaflyza Marbukhari [4]

Nur Nabila Mohamed [5]

[1-5]Faculty of Electrical Engineering,

40450 UiTM Shah Alam,

Selangor, Malaysia.

[1]anuarls@hotmail.com (corresponding author)
[2]habib350@salam.uitm.edu.my
[3]syed_farid@salam.uitm.edu.my
[4]eijafly@gmail.com
[5]nurnabilamohamed@gmail.com

Abstract: Keyless Go, Automotive keyless systems (AKS), passive keyless entry and start (PKES) are names given to smart systems that allow a driver to unlock a car without pressing any key, and drive the car without inserting a smart key for starting or stopping the car engine. It is one of the debutant IoT applications in automotive sector. This work presents a 128-bit pairing security protocol (PSP 128 bits) lightweight cryptographic protocol as a security protocol authentication between owner and car. The PSP 128 security analysis in timing and relay attacks by an adversary will be discussed and its resilience proved using a theoretical security reduction method. The theoretical security reduction results are supported by findings from an experimental test bed using RaspberryPi board and radio frequency (RF) communication. Based on the experiment results, the PSP 128 can support up to 56 thousand authentication sessions between owner and car per typical usage. It is estimated that a standard automotive battery running the device can have a lifespan of up to 7 years with typical use.

Keywords: keyless; automotive; relay attack; side-channel attack; iot, lightweight; cryptography; rf security; raspberrypi.

Reference to this paper should be made as follows: Mohd Anuar Mat Isa, Habibah Hashim, Syed Farid Syed Adnan, Norhaflyza Marbukhari and Nur Nabila Mohamed. (2017) 'An Automobile Security Protocol: Side-channel Security against Timing and Relay Attacks', *Int. J. Electronic Security and Digital Forensics. Vol. xxxxxx, No. xxxxxx, pp.1–16.*

Biographical notes: Mohd Anuar Mat Isa is a former Researcher at MIMOS

Berhad since 2008 until 2011. He is a freelance researcher and involves in various research works. He is also a member of the Malaysian Society for Cryptology Research (MSCR). His research focuses on asymmetric cryptography, lightweight cryptography for embedded devices, embedded firmware security, formal methods, trust and mathematical modelling, international relations and trusted computing.

Habibah Hashim is an Associate Professor in the Faculty of Electrical Engineering at Universiti Teknologi MARA (UiTM) and has served as the Deputy Dean of Research and Industrial Linkages between 2011 to 2014. Currently she is heading the Information Security and Trusted Information Laboratory and is pursuing her research interests in wireless and mobile networks, data communications, secure and trusted systems, internet of things, cloud computing and e-health systems.

Syed Farid Syed Adnan is an academic staff at UiTM since 2009. His research works focus in bioinformatics, cryptography and information security.

Norhaflyza Marbukhari is a master student at UiTM. Her research works focus on information security and wireless sensor network security.

Nur Nabila Mohamed is a PhD student at UiTM. Her research works focus on lightweight cryptography and information security.

1 Introduction

Automotive keyless systems (AKS), passive keyless entry and start (PKES) systems are some of IoT's latest applications for the automotive sector. They provide a smart authentication protocol between owner (by key) and car. The smart authentication protocol employed in these systems are based on various standard cryptographic protocols and random number generation. However, the standard cryptographic protocols are designed to harden private messages by encryption, which changes the private messages into ciphertexts. Most of the standard cryptographic protocols are hard to break (decipher) without private keys.

Interestingly, the primary security threat in AKS is not an attack to break the ciphertexts, but rather to fool the AKS through schemes that are based on side-channel attacks. However, it is important to note here that side-channel information such as leaked cryptographic secrets originating from decryption runtime and energy consumption (Kocher, 1996), and cryptographic communication protocol runtime data (Mohd Anuar Mat Isa et al., 2015a) can also be useful in attacks. Nevertheless, relay attacks are the main side-channel security threat to owners of luxurious and expensive cars (Francillon et al., 2011). In consideration of the aforementioned facts, we believe that any defence mechanism for security systems such as AKS should consider timing in the mitigation of relay attacks.

To mount a relay attack, an attacker will set up a radio frequency (RF) relay between the owner and car, which will act as a man-in-the-middle during a security authentication session. The relayed security authentication credentials will authorize a car (to unlock/lock) even though the car's owner is closer to the car. This is what is meant by fooling the AKS using relay attacks. There is no attempt to break cryptographic

encryption key, but through relaying of the sensitive RF communication data between owner and car, enable the attackers to capture secret information related to the operation of the AKS system

This work presents PSP 128 bits cryptographic protocol as a security authentication protocol between owner and car. The PSP 128 security for timing and relay attacks will be discussed and proved using a theoretical security reduction and experimental testbed. This paper is organized as follows: This section provides an introduction to AKS and relay attacks. Section 2 will discuss the state of the art in AKS technology and relay attack methods. Following this, the next section will revisit PSP cryptographic protocol while section 4 will provide a description of the experimental testbed and its configurations which use DenX U-Boot in RaspberryPi B+ (RPi) board. Section 5 will present results obtained from tests conducted on the experimental testbed, which includes power consumptions and performances of the PSP 128 cryptographic scheme in consideration of RF and Ethernet communications support, and PSP 128 endurance and lifespan when used with a standard automotive key battery. Section 6 presents security analysis concerning on an indistinguishability adversary model and relay attack. Section 7 concludes the research work done by the authors and also offers an introduction to a future work.

2 Related Work

We have revisited previous literature relating to AKS, timing and relay attacks, countermeasures for timing and relay attacks, and the most recent related works (Mohd Anuar Mat Isa et al., 2015b, 2015c, 2014a, n.d.; Mohd Anuar Mat Isa and Habibah Hashim, 2014) by this publication authors. This publication will focus on automotive security rather than cryptographic works because we had discussed many cryptographic related literature in our previous works. P. Nisch (Nisch, 2011) surveys 14 security threats in modern automotive systems such as no message authentication and input validation in Engine Control Unit (ECU), spoofing, relay attacks etc. The author also cited Francillon (Francillon et al., 2011) who found that ten cars from eight well-known brands have been hacked using the relay attacks. Francillon (Francillon et al., 2011) from ETH Zurich have shown practical experiments used to fool AKS through relay attacks using large timing delays for long distances and multiple relays for radio-hopping relays for long distances. Both (Francillon et al., 2011; Nisch, 2011) also discuss on exploiting other sensors in the car such as brakes, lights, diagnosis devices etc. for other types of attacks. Other works (Alrabady and Mahmud, 2003; Boureanu et al., 2014; Hoppe et al., 2011; Moradi and Kasper, 2009; Yang et al., 2012) also discuss similar topics but they did not provide experimental results to support their arguments. Khan (Khan, H.N., Chaudhuri and Kar, S., Roy, 2015) and Jin (Jin, C., Xu, C., Zhang and and Li, 2015) also discussed efficient methods to provide security authentication.

A. Francillon et al. (Francillon et al., 2011) discussed countermeasures of relay attacks which include using a physical or software shielding mechanism for the key whenever it is not being used. Removing key batteries or power control switches for keys, access control restrictions, relay detection based on radio strength between key and car, and unique signal modulation properties to detect demodulated signal by an attacker for relay radio retransmission. The authors also suggested a distance bounding method by

measuring upper-bound distance bounding between key and car, which detects closer distances for two legitimate parties and also detect further distances for attackers. This method explores processing times of round-trips between the key and car, which is also implemented in this work. Comparing to the Francillon (Francillon et al., 2011) work, this work integrates a lightweight PSP cryptographic protocol with timing analysis in the detection of possible relay attacks; and furthermore by a theoretical security reduction method together with experimental results, this work has tested and proved the reliability of the PSP cryptographic protocol (PSP 128) in mitigating timing and relay attacks. We conducted an energy feasibility study of the protocol for automotive key security for further proof of its lightweight properties.

3 PSP Protocol

This section will discuss a chained session key for PSP protocol (Mohd Anuar Mat Isa et al., 2015c, 2014a). The chained session key is used for establishments of secure session keys for every communication between owner and automotive (e.g. car). Hardware setup for an implementation of the PSP protocol will be discussed in section 4. Figure 1 shows an overview of PSP protocol, which consists of three stages. Stage 1 is used to establish the core root of trust key (CRT) between owner and car. Stage 2 is used to generate chained session keys for all communication between owner and car. Stage 3 is used to verify all keys that have been generated in Stage 2. If a new session key happens to fail in the Stage 3, all temporary session data will be flushed, and new data will be generated for reestablishment a new session key.

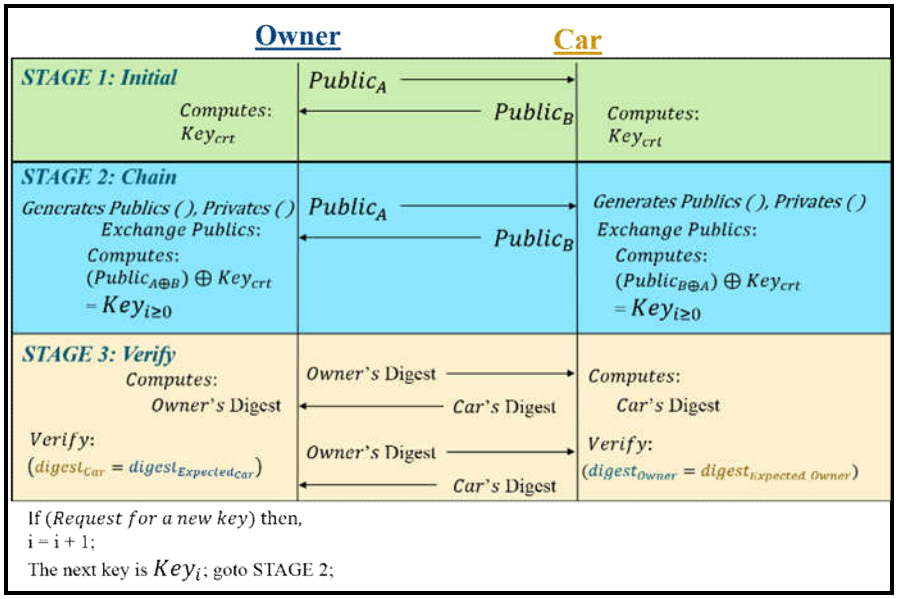

Figure 1. An overview of PSP protocol

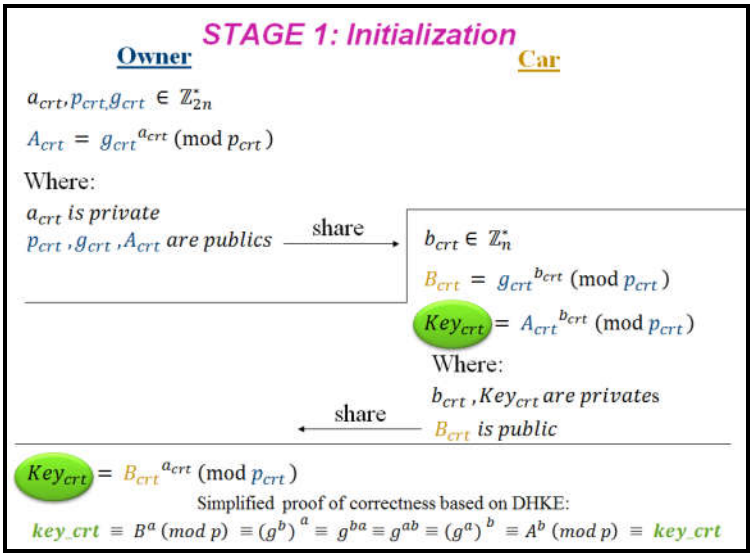

Figure 2. Stage 1: Initialization of core root key for PSP

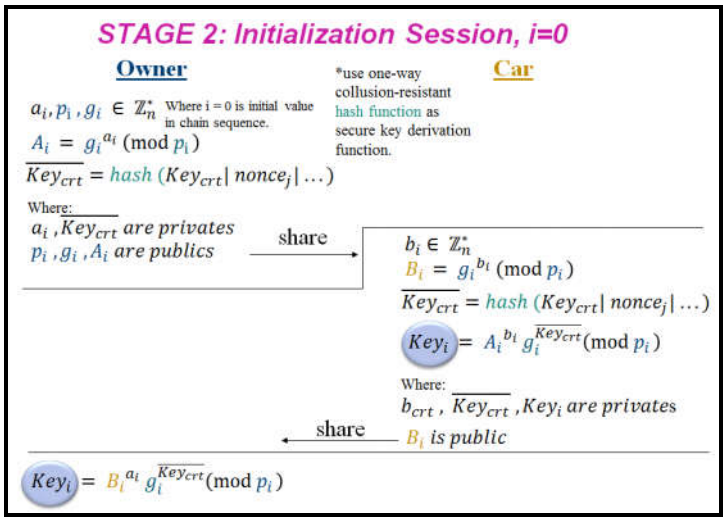

Figure 3. Stage 2: Initialization of PSP session

Figure 2 shows the details of Stage 1 cryptographic protocol. It is similar to DHKE for secret sharing between owner and car. Stage 1 is assumed to happen during manufacturing process or in a secure environment without the presence of any security threat. In this stage, both parties will share a longer secret key compared to the session keys in Stage 2. For an example, if the size of the Stage 2 session key is 128 bits, then the size of the core root key (CRT) should at least be double of the session key size,

wherein 256 bits in this example. The CRT should be a long key because if the Stage 2 session is vulnerable, it must be reset and the CRT key need to be used again for a new session key initialization. We expect that the CRT must be highly secure compared to the session key because it is a reusable key.

Figure 3 shows an initialization of PSP session using CRT hash. It will not use the CRT hash when session $i > 0$, but it will use a previous session key hash $\overline{Key_{i-1}} = hash\left(Key_{i-1} \mid nonce_j \mid ...\right)$. Stage 2 will produce the first session key $Key_0 = B_0^{a_0} g_0^{\overline{Key_{crt}}} \left(mod\ p_0\right) \equiv A_0^{b_0} g_0^{\overline{Key_{crt}}} \left(mod\ p_0\right)$ and subsequent session keys $Key_i = B_i^{a_i} g_i^{\overline{Key_{i-1}}} \left(mod\ p_i\right) \equiv A_i^{b_i} g_i^{\overline{Key_{i-1}}} \left(mod\ p_i\right)$. Every session key must be verified in Stage 3 as illustrated in Figure 4. Figure 4 shows hash digests of owner and car being verified by a mutual verification process. Both parties can generate and verify both hash digests if there exist a valid pairing between them. The pairing can only be established by knowing the previous session information using Key_{crt} or Key_{i-1}. One may refer to (Mohd Anuar Mat Isa et al., 2015c, 2014a) for a further discussion of PSP.

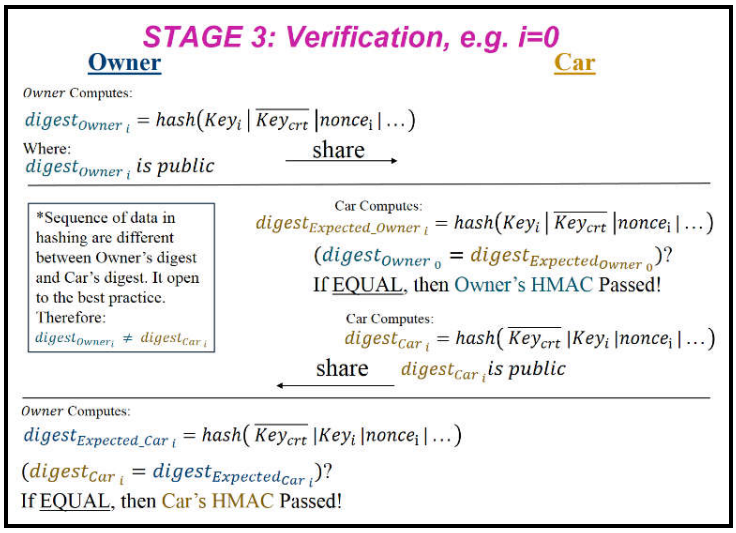

Figure 4. Stage 3: Verification of PSP session

4 Experimental Setup

This section describes the testbed for testing the lightweight automotive PSP using RaspberryPi B+ 700 MHz. We used three sets of RaspberryPi Boards and Texas Instruments C1110 RF modules. The RF modules operate using a built-in antenna (without an external antenna), which limits transmission distances to less than 10 meters. Each set was assigned as an owner, car and adversary respectively. Configuration for the owner and car is shown in Table 1. The adversary will act as a repeater (relay). To ensure

a reliable/stable radio quality between owner-car and owner-adversary-car setups, distances between all entities are set up in a straight line at 5 meters apart.

Table 1. Testbed configuration

Configurations	**Value**	**Command**
RaspberryPi B+ Voltage	5	NIL
icache off (Amp)	-0.009	icache off (in U-Boot)
dcache off (Amp)	-0.002	dcache off (in U-Boot)
RPi Board (icache+dcache) (Amp)	0.132	NIL
RF Module Power (Amp)	0.04	NIL
100Base RJ-45 Ethernet (Amp)	0.189	NIL
Run PSP 128 (Amp)	0.002	do_psd128 (in U-Boot)
2x Battery 80 mAH, ~5V	120	NIL
Serial Baud rates	115200	ATBD 1C200 (AT Command)
Radio Frequency (MHz)	915	ATCH 1 (AT Command)
Radio Frequency Channel Number	0	ATCN 0 (AT Command)
Radio Power Level (dBm)	10	ATPL 8 (AT Command)
Radio Rx to Tx transition delay (ms)	0	ATRT 0 (AT Command)
Radio Tx to Rx transition delay (ms)	0	ATTR 0 (AT Command)
Radio Data Rate (250 Kbaud)	250000	ATDR 1 (AT Command)
Radio Frame (bytes)	32	ATPK 20 (AT Command)
Radio Frame Timeout (ms)	16	ATRO 10 (AT Command)

The experiment was conducted using DENX U-Boot(DENX Software Engineering, 2016), a universal boot loader or firmware for embedded systems. The U-Boot version from DENX's repository is U-Boot-2015.10-rc3.tar.gz. It was added to PSP 128, compiled and loaded onto an SD card. To implement cryptographic primitive computation in the U-Boot, GNU GMP's mini-gmp ("The GNU Multiple Precision Arithmetic Library," 2014) library version gmp-5.1.0 had been ported into U-Boot as discussed in the previous work (Mohd Anuar Mat Isa et al., 2014a). Figure 1 shows a snapshot of *do_psd128* command with *icache* and *dcache* enabled in U-Boot console.

```
U-Boot 2015.10-rc3 (Mar 22 2016 - 01:26:28 +0800)

DRAM:  448 MiB
RPI Model B rev2
MMC:   bcm2835_sdhci: 0

U-Boot>icache on
U-Boot>icache
Instruction Cache is ON
U-Boot>dcache on
U-Boot>dcache
Data (writethrough) Cache is ON
U-Boot> do_psd128
PSP 128
Raw Platform Tick Total:      1983706   Start:1095275853
End:1097259559
```

Figure 5. A snapshot U-Boot during experiment

5 Results and Discussion

This section will present results and discussion of PSP 128 experiments ran between owner and car. The experiments were set up to perform four different measurements, which are cryptographic performances, network communication, session performance and battery sustainability metrics. Table 1 shows the results of PSP cryptographic performances with four CPU configurations. The outcome of this experiment has shown that PSP which enabled either *icache*, *dcache* or both in CPU have significantly improved PSP computation speeds by at least five times.

Table 3 shows the network communication performances for one PSP session using RF module and 100 Base Ethernet. RF communication uses serial RS232 as an interface between the RF module and RPi board. The low bandwidth capability of serial and RF module causes slow data rates for the RF communication compared to wired Ethernet. Based on the Table 3, the 100 Base Ethernet outperforms the RF communication, wherein 100 Mbps is superior than 250 Kbps + 115.2 Kbps (RF + serial). When a communication medium is slow, it will keep RPi board operational during communication, which it will drain more energy. That is the main reason for a huge power consumptions gap between RF and Ethernet.

Table 2. Cryptographic performance of PSP 128

Cryptographic Scheme: PSP 128	**PSP CPU Ticks**	**PSP Runtime (Seconds)**	**PSP + RPi Board (watt)**
Instruction & Data Caches: ON	1983706	0.0079348	0.0052391
Instruction Cache: Off Data Cache: ON	10425922	0.0417038	0.0294129

Instruction Cache: ON Data Cache: OFF	12620795	0.0504833	0.0338373
Instruction & Data Caches: Off	15728826	0.0629154	0.0450025

Table 3. Total runtime and power consumption in communication

Communication: PSP 128	**Value**
Serial Data Rate (seconds)	0.267130435
Radio Data Rates (seconds)	0.012288
Ethernet Data Rates (seconds)	0.00000318
Serial + Radio + RPi Board (watt)	0.04582019
Ethernet 100 Base + RPi Board (watt)	0.00001020

Table 4. Total power consumption for two parties' communication (complete one session)

Communication Protocol: PSP 128	**PSP + RPi Board + RF Modules (watt)**	**PSP + RPi Board + Ethernet (watt)**
Instruction & Data Caches: ON	0.3685566	0.1962411
Instruction Cache: Off	0.3927304	0.2204150
Data Cache: OFF	0.3971548	0.2248394
Instruction & Data Caches: Off	0.4083200	0.2360046

Table 4 shows the total energy consumption for one owner-car PSP session. The results have shown that PSP over Ethernet is almost two times faster than PSP over RF. However, for the actual implementation, in practice no one will use wired communication for this purpose because AKS operate over RF. Table 5 and Figure 6 show an execution of PSP using a standard automotive car key battery. When *icache* and *dcache* are turned-on, it has been demonstrated that PSP computations improved drastically. Similarly, a high-speed communication Ethernet medium also contribute to increasing the usability of PSP sessions and a reduction in battery consumption as depicted in Table 5. In this work, we only used the PSP over Ethernet as a performance benchmark, which does not render it as a practical solution given that AKS operates over RF. Based on the experimental results in Tables 2 to 5, PSP runtime is less than 0.3 second and it can sustain PSP sessions for 56,405 times before 2x 80 mAh batteries deplete in RF environment. The results show that PSP 128 is feasible to be deployed in AKS.

Table 5. PSP 128 usage using 2x80 mAH batteries

PSP 128 Overall Performance	PSP on RPi Board + RF Modules using 2x 80 mAh Batteries	PSP on RPi Board + Ethernet using 2x 80 mAh Batteries
Instruction & Data Caches: ON	56,405	425,730
Instruction Cache: Off	38,281	77,028
Data Cache: OFF	36,154	66,222
Instruction & Data Caches: Off	31,710	50,500

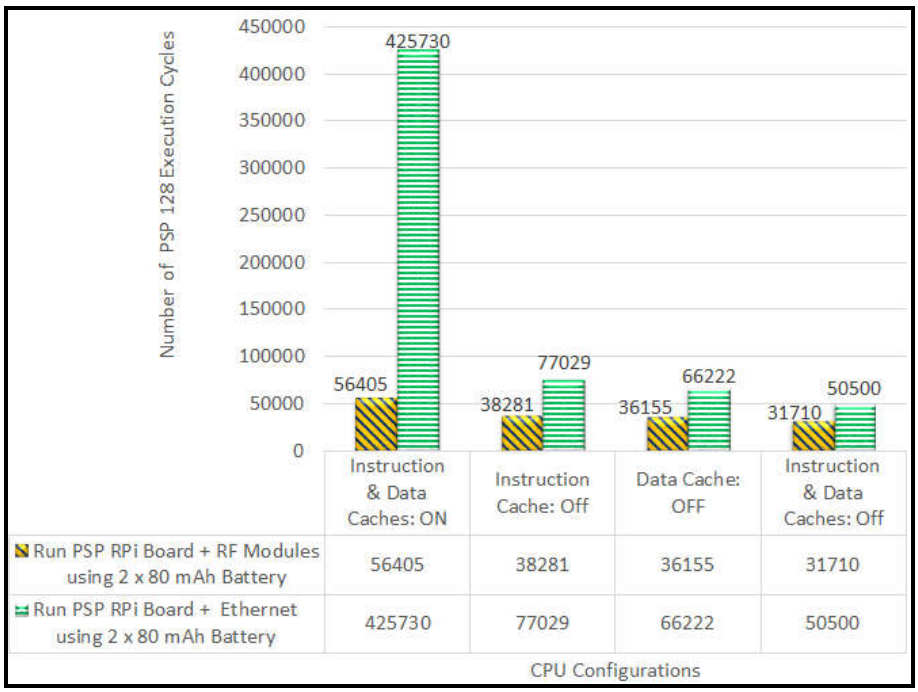

Figure 6. PSP 128 execution cycles using 2x 80 mAh batteries

6 Security Analysis

This section will present the security analysis of PSP 128. We divided it into two parts of adversary models: 1) Indistinguishability-Adaptive Chosen-Ciphertext with Timing and Relay Attacks (IND-CCTRA). The results in Tables 2-5 used longest bits of private and public parameters, which will produce a worse case of PSP 128 session execution duration. We have chosen a worst case runtime of the PSP 128 session as a baseline for all the PSP 128 sessions. If any PSP 128 session key computation does not complete by the time stipulated in Security Assumption 5 **(SA 5)**, it will be regarded as a relayed key

and should be duly discarded, and the algorithm deemed to be not secure against a relay attack.

IND-CCTRA is an attack that allows an adversary to access identical computing resources in terms of computing performance (e.g. CPU, network etc.). The adversary is given knowledge of time to perform cryptographic computations (e.g. primitive computation and protocol execution). The adversary can also get access data pertaining to delay of network transmission for all transactions in Phase 1, Phase 2 and Challenge phase as shown in Figure 7. Messages m_0 and m_1 will be encrypted by the challenger. The challenger then returns the computation time for both messages as t_{m0}, t_{m1} to adversary with a random ciphertext c^*. Either an encryption time of t_{m0} or t_{m1} is the actual time for the ciphertext c^* was computed. By the knowledge of t_{m0}, t_{m1} ; can the adversary gains a non-negligible *advantage* to distinguish the challenge's ciphertext c^* in a polynomial time? One may refer to previous works of (Mohd Anuar Mat Isa et al., 2015a, 2015c, 2014a, 2014b) for detailed discussions on CPA, CCA1, CCA2, IND-CCTA2 etc. The previous works had also discussed PSP security against a session state reveal attack, forward secrecy, key independence and key derivation function attack. The following will demonstrate a security analysis of IND-CCTRA.

Adversary Model: IND (CPA, CCA1, CCA2), Timing and Relay Attacks or IND-CCTRA

Adversary Knowledge: E, D, $c_i, m_i, t_i, t_{m_0}, t_{m_1}, c^*$

Adversary Limitation: Outsider attack, Protocol Π is protected/sealed using temper resistance device (but an adversary succeeds to capture all network frames/packets (wired or wireless) with precision of time in/out to the sealed box of Protocol Π during runtime or idle)

Adversary Goal: successfully distinguish a challenge ciphertext c^* with higher probability ε

Security Assumption (SA):

1. Any attempt by an adversary to perform a store and forward RF frame will produce a communicating delay between owner and car as presented in Figure 8.
2. Based on the experiment, when an adversary performs relay attacks, it will cause the communication delay (**SA 1**) by greater than $(radio\ data\ rates + \frac{radio\ data\ rates}{2})$. One may refer to Table 3 for the radio data rates.
3. Fixed-time PSP session runtime is assumed as a fixed input length in a polynomial time function, wherein the function that receives any valid input of the same length (e.g., *f(101)* and *f(001)*, where |*f(101)*|=|*f(001)*|) is assumed to have identical runtime or execution time for all conditions. The fixed-time value will be based on the worst-case scenario to compute the PSP session runtime.
4. Hash function is a universal one-way hash function with strong collision-resistant (Cramer and Shoup, 1998; Tsudik, 1992).

5. Computational Diffie-Hellman (CDH) problem in a cyclic group G is hard to solve (Boneh, 1998) in a time less than or equal to the fixed-time (**SA 3**) and PSP session key will expired after the *fixed-time* + $(radio\ data\ rates + \frac{radio\ data\ rates}{2})$ or more (**SA 2**).

If SA 1 until 5 are true; then PSP 128 encryption scheme is secure against IND-CCTRA using indistinguishability test.

Reductionist Security Claim: Anyone who can read message m from a ciphertext c^* must also be able to solve CDH problem in **SA 5** and also be able to reverse the one-way hash function **SA 4** in terms of collusion resistance property.

Security Reduction Experiment: An adversary claims that he can break PSP protocol using efficient methods in less than or equal to the time specified in **SA 5**. The adversary is then considered the winner in the experiment, if the probability to guess for all correct messages are non-negligible with an advantage of $\left(\frac{1}{2}\right)+\varepsilon(n)$, where $\varepsilon(n)$ is the adversary's success probability. Otherwise, if the probability to guess results in a negligible advantage to break the PSP protocol by the **SA 5**, then the PSP protocol wins the experiment due to the negligible advantage of the adversary. Based on **SA 4 and SA 5**, the adversary's advantage over probabilistic polynomial-time[1] is negligible due to the adversary's inability to distinguish whether the ciphertext c^* was either m_0 or m_1 within the conditions stipulated by **SA 4 and SA 5**.

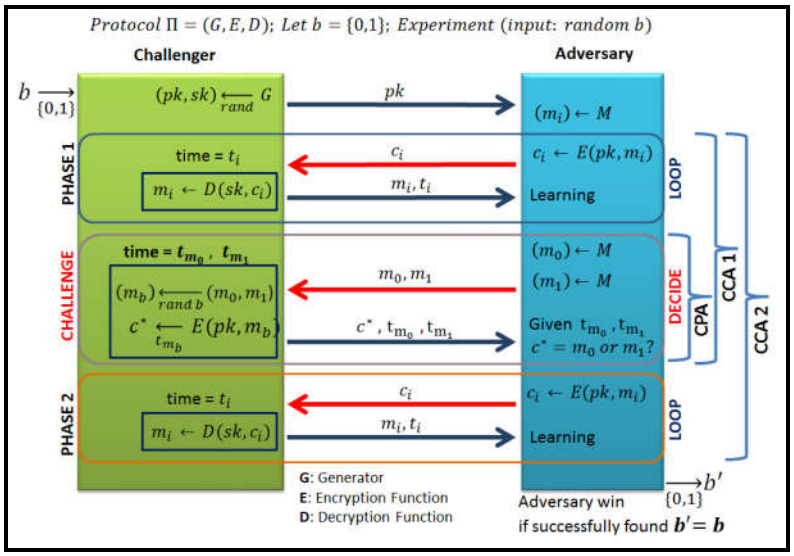

Figure 7. Adversary Model: Indistinguishability-Adaptive Chosen-Ciphertext and Timing Attacks (IND-CCTRA)

[1] "polynomial-time" is a term for measuring an algorithm's running time as a function, wherein it is measured by length of its input into the function.

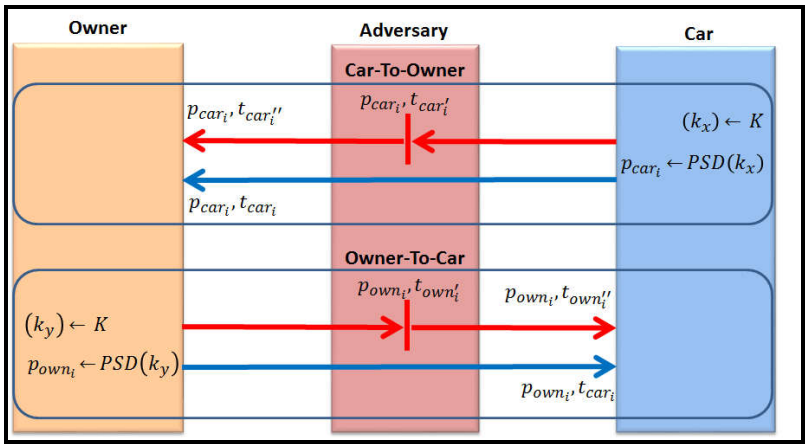

Figure 8. Relay Attacks in IND-CCTRA

7 Contributions

This paper contributes an implementation of PSP protocol in AKS. We have demonstrated its practicality as a lightweight protocol for the AKS. Based on the experiment results, PSP 128 sessions can run up to 56,405 authentication sessions between owner and car in the specified battery lifespan. It can save 1.5 years of battery power for a daily usage of 100 sessions per day or 7.7 years for 20 sessions per day. Based on the given lifespan, PSP 128 is feasible protocol be applied in the AKS to mitigate timing and relay attacks. The PSP 128 can also be used in Wireless Sensor Networks (WSN) for a lightweight sensor node authentication for secure IoT communication. It can provide anonymous identities (for privacy enhancement) between sensors using a unique PSP session key for every session authentication. Furthermore, the unique PSP session key and chained session keys can prevent node cloning in WSN systems. Other promising applications for the PSP 128 is secure biomedical sensors for smart healthcare, secure remote system updates for structural health monitoring (SHM), and secure IoT systems in building (e.g. malls, shopping complexes, government offices), smart homes etc.

Referring to the experiment setup and the results obtained, we have shown that an adversary would have failed to perform timing and relay attacks for short distances (e.g. 5 meters between owner and car). The owner's eye visibility should be clear within 10 meters to see the car, yet we have shown that the adversary had failed to intercept PSP sessions authentication. Therefore, any attempt by the adversary to steal or open the car from more than 10 meters can reasonably be expected to fail. Additional relay adversaries will also generate more store and forward RF frames, and this will introduce more delays, which would not fool the PSP sessions authentication protocol as it would have detected the relay attack in due course.

We have also presented a security proof using a semi-formal notation for an adversary model and security reduction technique. We have proposed a novel IND-CCTRA adversary model and reduction security proving that can be used in an

international standard such as Common Criteria's Evaluation Assurance Level 6 (EAL6) (Common Criteria, 2014). Leading countries such as the USA, UK, German, France etc. requires that any IT security product is certified by at least EAL1 before it can be consumed (Common Criteria, 2014). The EAL6 consents a semi-formal verified design and security test for target systems (e.g. a lightweight automotive keyless system proposed by this work).

8 Conclusion

We have performed an experiment and security analysis to demonstrate PSP deployment for a lightweight automobile keyless system. The outcome has shown that it is able to resist adversary attacks by timing and relay attacks by way of IND-CCTRA indistinguishability test. We have also proposed a variety of PSP applications for WSN, IoT, structure health monitoring (SHM), healthcare etc. in the Contributions section. We have provided security proofs and a security compliant to Common Criteria's EAL6 for the lightweight automobile keyless system using PSP 128. For a future work, we will setup testbeds for various ARM Cortex-M microcontrollers. The future work will provide feasibility studies of the PSP 128 and PSP 256 for energy efficiency, cryptographic computation and the IND-CCTRA.

9 Acknowledgement

The authors would like to acknowledge the Ministry of Education (MOE) Malaysia for providing research grants: PRGS and FRGS; and Universiti Teknologi MARA (UiTM) for supporting this research work.

10 References

Alrabady, A.I., Mahmud, S.M., 2003. Some attacks against vehicles' passive entry security systems and their solutions. IEEE Transactions on Vehicular Technology 52, 431–439.

Boneh, D., 1998. The decision diffie-hellman problem. In: Algorithmic Number Theory. pp. 1–14.

Boureanu, I., Mitrokotsa, K., Vaudenay, S., Polytechnique, É., 2014. Towards Secure Distance Bounding. Lecture Notes in Computer Science 8424, 55–67.

Common Criteria, 2014. Arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security.

Cramer, R., Shoup, V., 1998. A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack. In: Lecture Notes in Computer Science: Advances in Cryptology—CRYPTO'98. pp. 1–18.

DENX Software Engineering, 2016. Denx U-Boot. URL http://www.denx.de/wiki/U-Boot/SourceCode (accessed 4.19.16).

Francillon, A., Danev, B., Capkun, S., 2011. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. Network and Distributed System Security Symposium 431–439.

Hoppe, T., Kiltz, S., Dittmann, J., 2011. Security threats to automotive CAN networksPractical examples and selected short-term countermeasures. In: Reliability Engineering and System Safety. pp. 11–25.

Jin, C., Xu, C., Zhang, X., and Li, F., 2015. An efficient certificateless deniable authentication protocol without pairings. Int. J. Electronic Security and Digital Forensics, Vol 7, 179–196.

Khan, H.N., Chaudhuri, A., Kar, S., Roy, P. and C., 2015. Robust symmetric cryptography using plain-text variant session key Hari Naray. Int. J. Electronic Security and Digital Forensics, Vol 7, 30–40.

Kocher, P., 1996. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Advances in Cryptology—CRYPTO'96.

Mohd Anuar Mat Isa, Habibah Hashim, 2014. Adversary Model : Adaptive Chosen Ciphertext Attack with Timing Attack. In: arXiv:1409.6556 [cs.CR]. pp. 1–3.

Mohd Anuar Mat Isa, Habibah Hashim, Jamalul-lail Ab Manan, Syed Farid Syed Adnan, Ramlan Mahmod, 2014a. An Experimental Study of Cryptography Capability using Chained Key Exchange Scheme for Embedded Devices. In: Lecture Notes in Engineering and Computer Science. pp. 510–515.

Mohd Anuar Mat Isa, Habibah Hashim, Jamalul-lail Ab Manan, Syed Farid Syed Adnan, Ramlan Mahmod, 2015a. Cryptographic Adversary Model: Timing and Power Attacks. Transactions on Engineering Technologies, Springer.

Mohd Anuar Mat Isa, Habibah Hashim, Syed Farid Syed Adnan, Jamalul-lail Ab Manan, Ramlan Mahmod, n.d. A Secure TFTP Protocol with Security Proofs. In: Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering 2014, WCE 2014, 02-04 July, 2014, London, UK. pp. 443–448.

Mohd Anuar Mat Isa, Hashim, H., Adnan, S.F.S., Manan, J.-L.A., Mahmod, R., 2014b. A secure TFTP Protocol with security proofs. In: Lecture Notes in Engineering and Computer Science. pp. 443–448.

Mohd Anuar Mat Isa, Hashim, H., Ghafar, A.H.A., Manan, J.A., Adnan, S.F.S., Mahmod, R., 2015b. Cryptographic Adversary Model: Timing and Power Attacks. In: Transactions on Engineering Technologies: World Congress on Engineering and Computer Science 2014. pp. 193–207.

Mohd Anuar Mat Isa, Hashim, H., Manan, J.A., Adnan, S.F.S., Mahmod, R., 2015c. A Series of Secret Keys in a Key Distribution Protocol. In: Transactions on Engineering Technologies: World Congress on Engineering and Computer Science 2014. pp. 193–207.

Moradi, A., Kasper, T., 2009. A new remote keyless entry system resistant to power analysis attacks. ICICS 2009 - Conference Proceedings of the 7th International Conference on Information, Communications and Signal Processing.

Nisch, P., 2011. Security Issues in Modern Automotive Systems.

The GNU Multiple Precision Arithmetic Library, 2014. URL http://gmplib.org/

Tsudik, G., 1992. Message authentication with one-way hash functions. ACM SIGCOMM Computer Communication Review 22, 29–38.

Yang, T., Kong, L., Xin, W., Hu, J., Chen, Z., 2012. Resisting relay attacks on vehicular Passive Keyless Entry and start systems. In: Proceedings - 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, FSKD 2012. pp. 2232–2236.