*September 20, 2014. Submitted for publication*

# ON KLJN-BASED SECURE KEY DISTRIBUTION IN VEHICULAR COMMUNICATION NETWORKS

*X. Cao [1,3], Y. Saez [1,+], G. Pesti [2], L.B. Kish [1]*

*[1] Department of Electrical Engineering, Texas A&M University, College Station, TX 77843-3128, USA*
*yessica.saez@tamu.edu; laszlo.kish@ece.tamu.edu*

*[2] Texas A&M Transportation Institute, Texas A&M University, College Station, TX 77843-3135, USA*
*g-pesti@tamu.edu*

*[3] College of Automotive Engineering, Jilin University, Changchun, Jilin 130025, China*
*caoxiaolin@jlu.edu.cn*

Received (received date)
Revised (revised date)
Accepted (accepted date)

In a former paper [*Fluct. Noise Lett.*, **13** (2014) 1450020] we introduced a vehicular communication system with unconditionally secure key exchange based on the Kirchhoff-Law-Johnson-Noise (KLJN) key distribution scheme. In this paper, we address the secure KLJN key donation to vehicles and give an upper limit for the lifetime of this key.

*Keywords:* Security; Vehicular Communication Networks; Kirchhoff-Law-Johnson-Noise (KLJN); Unconditional Security.

## 1. Introduction

After more than 100 years of development on modern vehicle technology, we are on our way to smarter cars and much more intelligent transportation systems. Nowadays, people pay more attention to safety and comfort in vehicles, rather than traditional traction ability, fuel cost, handling, and stability. Therefore, it is believed that safety and mobility information such as road and traffic information (e.g. emergency braking, vehicle collision, congestion, toll collection, etc.), weather forecast warnings (e.g.

[+] Corresponding Author, *yessica.saez@tamu.edu*

water or ice on the pavement) and local services (e.g. route maps, gas or restaurant locations, etc.)[1–4] should be collected and provided to drivers and passengers in the vehicle.

### 1.1. *Vehicular Communication Networks*

Vehicular communication networks have become a reasonable intelligent transportation solution that can satisfy these demands effectively. A typical vehicular communication network is shown in Fig. 1[1, 5–9].

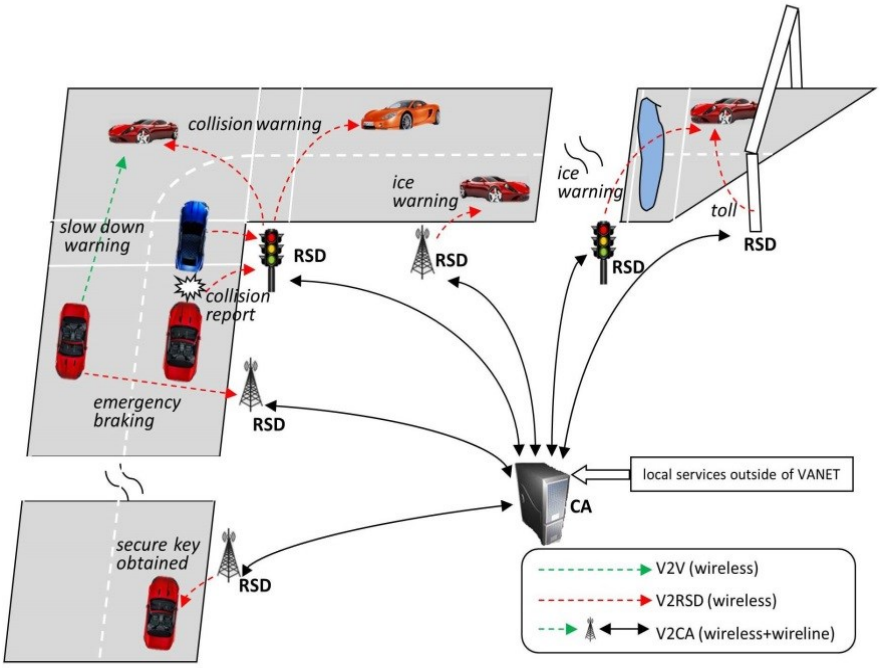


Fig. 1. A typical vehicular communication network. Three basic nodes are encountered in this type of network: Vehicles, Roadside Devices (RSDs) and Certification Authorities (CAs). The types of communication within vehicular communication networks include [1, 5–9]: Vehicle-to-Vehicle (V2V), Vehicle-to-Roadside-Device (V2RSD), and Vehicle-to-Certification-Authority (V2CA).

As summarized in previous publications [1, 5–9], Vehicles, Roadside Devices (RSDs) and Certification Authorities (CAs) are the three basic nodes in most of vehicular communication networks. Vehicles are mobile terminal nodes that are in charge of collecting road and traffic information, reporting events to the CAs through the RSDs, and exchanging warnings with nearby vehicles. The RSDs are intermediate nodes in charge of transferring messages between vehicles and CAs in two-ways. The

CAs are the host nodes that manage information related to vehicles. These nodes also generate secure keys and provide certifications for all vehicles in the network, control message exchanges of the whole network, and distribute local information obtained outside the local vehicular communication network. Accordingly, the types of communication within vehicular communication networks include [1, 5–9]: Vehicle-to-Vehicle (V2V), Vehicle-to-Roadside-Device (V2RSD), and Vehicle-to-Certification-Authority (V2CA). Communications within vehicular communication networks raise concerns for security and privacy. For example, the identity of vehicles, emergency braking, and vehicle collision warnings among vehicles must be transmitted securely to avoid malicious activities. The private financial information used in toll collection when cars pass by RSDs also needs to be protected.

In order to solve these fundamental security-related issues for promising vehicular communication network applications, several security protocols have been proposed by different researchers. In [10–11], the authors proposed a security infrastructure that is based on public key infrastructure (PKI). Later, other solutions based on PKI were proposed [2, 4, 12, 13]. The authors of [2] provided a "lightweight" authenticated key scheme that integrates blind signature techniques for V2V and V2RSD communications. In [4], the authors presented an approach that combines the traditional PKI and identity-based public key cryptography for vehicular communication networks. In [12], a secure scheme with session keys (pairwise and group keys) used in non-safety-related applications (e.g. "chatting in platoon") was designed. In [13], temporary anonymous certified keys (TACKs) were constructed, and a key management scheme based on TACKs was proposed for vehicular communication networks. Besides PKI, group signatures are another important category of proposed security methods. Based on the strong Diffie-Hellmanand linear assumptions, the authors of [14] introduced the under-200 bytes group signature scheme that has a similar security level to the RSA (Rivest, Shamir, and Adleman public-key cryptosystem) signature of the same length. A group signature based protocol using tamper-resistance devices and a probabilistic signature verification scheme was proposed in [3]. In [15], the authors constructed an identity-based batch verification scheme for V2RSD communication in vehicular communication networks. In [16], a software–based roadside unit-aided messages authentication protocol for V2V communications was proposed. In addition, a software-based solution that uses secure and privacy enhancing communication schemes for vehicular sensor networks was provided in [17].

Most of the above security schemes or protocols are constructed based on software encryption mechanisms. The security on these software-based methods is based on the

premise that the eavesdroppers have *limited computational power*. Thus, these security schemes offer just a *computationally conditional security* [18–22]. Moreover, these architectures focus their attention on V2V or V2RSD communications and although there is significant information transmitted in the Road-side-Device-to-Certification-Authority (RSD2CA) communication [9], it is very rare to find works related to securing this particular communication channel.

In [9], a novel, unconditionally secure vehicular communication architecture that utilizes the KLJN key distribution scheme was proposed. In this architecture, a new node called the Roadside-key-Provider (RSKP) was introduced to provide the cars with KLJN keys. Based on this work, we discuss the KLJN-based secure key generation, donation, and lifetime in vehicular communication networks. The remainder of this paper is organized as follows. In section 1.2, the working principle of the KLJN system will be discussed. In section 2, we discuss the key generation process in vehicular networks and propose a KLJN key donation solution for the vehicular communication architecture proposed in [9]. We also compute an upper limit for the KLJN key lifetime in vehicular communication networks.

### 1.2. *On the KLJN key exchange*

The illustration of the ideal KLJN key exchange scheme is shown in Fig. 2 [19, 21–24].

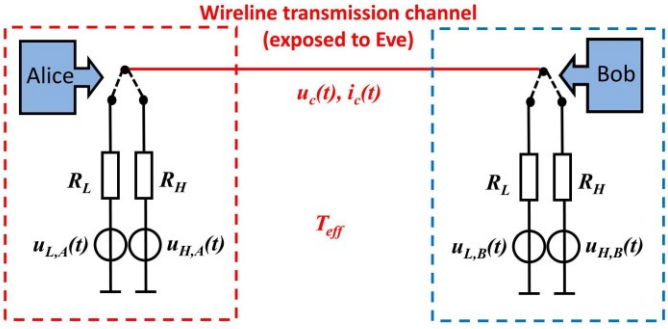


Fig. 2. Illustration of the ideal KLJN key distribution scheme. There is a switch and identical pairs of resistors ($R_L$ and $R_H$, $R_L \neq R_H$) on each communicator (referred to as Alice and Bob) side, where $R_L$ represents the low, $L$ bits , $R_H$ represents the high, $H$ bits; $u_{L,A}(t)$, $u_{H,A}(t)$ and $u_{L,B}(t)$, $u_{H,B}(t)$ are the Johnson noise voltages (Gaussian noise voltage generators) at temperature $T_{eff}$ of $R_L$ and $R_H$ of Alice and Bob, respectively, $u_c(t)$ is the channel noise voltage, and $i_c(t)$ is the noise current in the wire.

The Kirchhoff-law-Johnson-noise (KLJN) secure key exchange scheme was proposed in 2005 [19] as a statistical/physical competitor to quantum key distribution (QKD) [20]. The KLJN scheme provides unconditional security based on the Kirch-

hoff's loop law and the fluctuation-dissipation theorem [19, 21–24]; for a general security proof, see [25]. Several potential applications have been proposed such as: classical networks [26], smart power grids [27], secure computers, algorithms, and hardware [28].

In this ideal KLJN scheme, the two communicating parties, Alice and Bob, communicate via a wireline channel. There is a switch and identical pairs of resistors ($R_L$ and $R_H$, $R_L \neq R_H$) on each communicator side, where $R_L$ represents the low, $L$ bit and $R_H$ represents the high, $H$ bit. The $u_{L,A}(t)$, $u_{H,A}(t)$ and $u_{L,B}(t)$, $u_{H,B}(t)$ are the Johnson noise voltages at temperature $T_{eff}$ of $R_L$ and $R_H$ of Alice and Bob, respectively, while the $u_c(t)$ is the channel noise voltage, and the $i_c(t)$ is the noise current in the wire. At the beginning of the bit sharing period, both Alice and Bob randomly choose one of the resistors ($R_L$ or $R_H$) and the corresponding Johnson noise voltage ( $u_{L,A}(t)$ or $u_{H,A}(t)$, $u_{L,B}(t)$ or $u_{H,B}(t)$, respectively) and connect them to the wireline. The possible permutations of the resistors connected to the channel will be: $LL$, $LH$, $HL$, and $HH$. In the cases of $LL$ or $HH$, the location of the resistors and the exchanged bits are publicly known, thus these bits are discarded [19]. On the other hand, $LH$ and $HL$ are secure bit exchange situations, because Eve cannot differentiate between the situations $LH$ and $HL$.

The security of the ideal KLJN scheme is based on the Second Law of Thermodynamics [19, 21–24], that is the difficulty to crack the ideal KLJN system is similar to that of to build a perpetual-motion machine of the second kind. In addition, the KLJN system is robust and not sensitive to vibrations [24], and is easy to be integrated on chips [28]. Based on the above core scheme, some advanced schemes were proposed to [23] enhance the speed of the KLJN system.

In order to protect against active (invasive) attacks (and also against passive attacks on non-ideal systems), the KLJN system continuously monitors or measures the instantaneous current and voltage at the two ends of the line [22]. These measurements are compared via an authenticated public channel. Therefore, any intruder causing changes in the circuitry, and thus affecting the instantaneous measurements, will cause an alarm to go off and Alice and Bob will discover the intrusion. This defense mechanism is illustrated in Fig. 3.

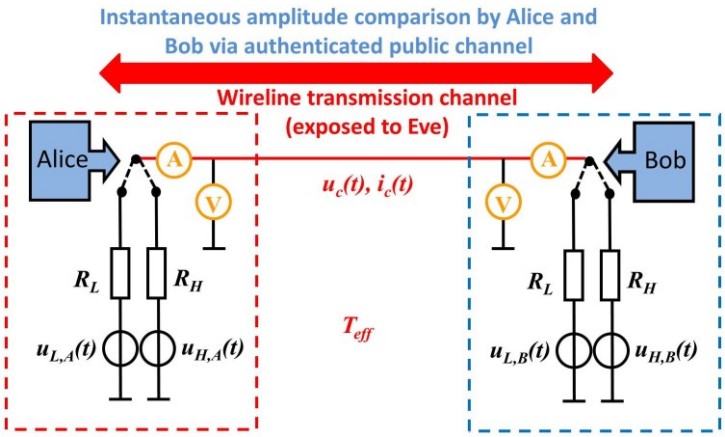


Fig. 3. KLJN system protection against invasive (active) attacks. Alice and Bob measure the instantaneous channel voltage and current amplitudes and compare them via an authenticated public channel. Alice and Bob learn all the information Eve can have. Additional elements to prevent hacking—such as line filters, line capacitance killer arrangement, etc.—are not shown. The notation is the same as in Fig. 2.

It is important to note that the instantaneous current and voltage data contain all the information related to the key that Eve could have. Thus, it is impossible for Eve to extract key information without letting the system know of such activity. In consequence, Alice and Bob can decide whether or not to discard the compromised bits according to a previously agreed maximum allowed level of information leak toward Eve [22].

According to the working principle of the KLJN scheme, the secure bit exchange takes place when the resistor states of the two communicators (i.e. the CA and RSD and/or RSKP in vehicular communication networks) are different, i.e. $LH$ or $HL$ .This is indicated by an intermediate level of the mean square noise voltage ($u_{msn}$) on the line, or that of the current noise in the wire [19]. This concept is shown in Fig. 4.

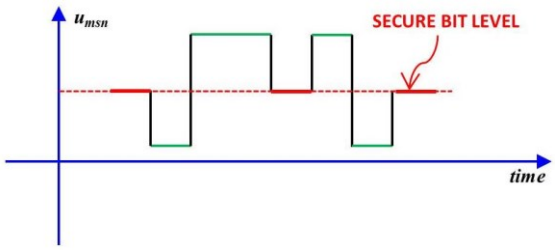


Fig. 4. The secure bit generation in the KLJN scheme. The intermediate mean square noise level represent the bit situations $LH$ or , that is when a secure bit exchange takes place.

It is important to mention that the two communication parties must previously and publicly agree on which one of them will invert the exchanged bit to have identical keys at the two ends.

## 2. KLJN Secure Key in Vehicular Communication Networks

Based on the working principle of the KLJN scheme [19] and the vehicular communication network model with unconditional secure key exchange proposed in [9], we discuss the generation, donation, and lifetime of the KLJN secure key in vehicular communication networks.

### 2.1. *KLJN key generation in vehicular communication networks*

According to the vehicular communication network model with unconditional secure key distribution proposed in [9], there is a KLJN line connecting the Certification Authority (CA) to the Roadside Devices (RSDs) and Roadside Key Providers (RSKP) (see Fig. 5).

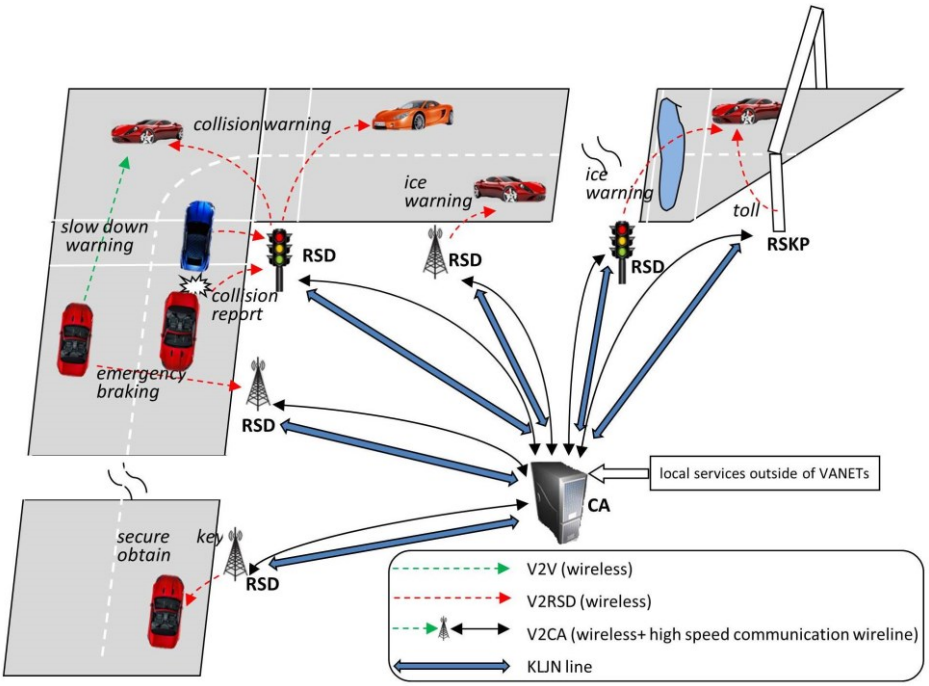


Fig. 5. Vehicular communication networks with unconditional secure key exchange. The network nodes remain the same except for a new node: the roadside key provider (RSKP) and extra wires for KLJN key exchange between the CA and RSD and/or RSKP. The existing wirelines between the RSDs/RSKPs and the CA are kept for high speed communication purposes.

The KLJN key generation process is performed as follows:

i). When a vehicle needs a secure key, it sends a message (via wireless communication) to the closest RSKP with the key request.

ii). The RSKP will use the extra wire (i.e. the high speed communication line) to inform the CA in charge about the key request.

iii). A key generation process will take place between the RSKP and the CA.

iv). The RSKP will then provide the cars with the unconditional secure keys by using a near field communication wireless technology [9].

v). The RSDs also use their KLJN lines that connect them to the CA to generate KLJN keys that are used to secure the communication between RSDs and the CA.

Note that the KLJN line is used only to secretly generate and share the KLJN keys that are going to be used to secure the communication between two nodes. The rest of the communication is done either via wireless communication or using a high speed communication wireline.

### 2.2. *KLJN key donation in vehicular communication networks*

It is important to mention that the RSKP key donation that was proposed in [9], where RSKPs were visualized as gates, might not be as efficient as expected. This is because vehicles would have to slow down in order to get sufficiently close to the RSKPs (as proximity is needed for secure key donation). Therefore, we also propose a lane-by-lane key donation using RSKP equipment embedded in the pavement. In this way, vehicles will not have to slow down to obtain their keys. To detect vehicles in each lane, either loop detectors [29] or high-definition digital wave radars [30] deployed on the side of the roadway can be used. Both the RSKPs and the radar units can be connected to RSDs through a high speed wireline connection. Thus, the KLJN key generation is performed between RSDs and the CA only, while the RSKP will be only in charge of providing the cars with the unconditionally secure KLJN keys. Moreover, this key donation process would be encrypted with the former key, therefore, even if an eavesdropper is listening, he/she would not be able to extract the key information unless he/she has the former key. Figure 6 illustrates this solution.

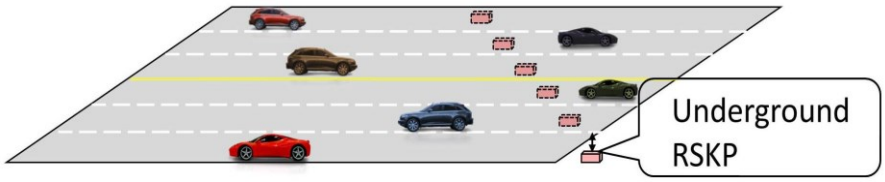


Fig. 6. Key donation with RSKP equipment embedded in the pavement. RSKPs are located underground of each lane.

### 2.3. *Upper limit of the KLJN key lifetime*

The lifetime of the KLJN key in vehicular communication networks is a very important technical parameter that needs to be discussed. This is because the longer the KLJN key is used, the more susceptible it is to attacks. In order to find out the lifetime of the KLJN key in vehicular communication networks, we proceed as follows.

First of all, the noise bandwidth $B_{KLJN}$ is determined by the distance $L$ between the two communicating parties, which in the case of vehicular communication networks depends on the length of the KLJN line segment between RSDs and the CA. Thus, the following relationship must be satisfied [19]: $L \ll \frac{c}{B_{KLJN}}$, where $c$ is the speed of electromagnetic waves in the wireline. Suppose that $0 < \Theta \ll 1$ and the noise bandwidth is:

$$B_{KLJN} = \Theta\frac{c}{L}. \tag{1}$$

Also, the duration of the bit sharing period, $\tau$, must be long enough compared to the correlation time, $\tau_{KLJN}$, of the noise, i.e., $\tau_{KLJN} \approx \frac{1}{B_{KLJN}}$, in order to correctly distinguish between the different resistors situations [31, 32]. The frequency of *secure* bit exchange is:

$$\mathrm{f_{sec}} = \frac{1}{2}\frac{B_{KLJN}}{\gamma}, \tag{2}$$

where $\gamma \gg 1$, see [31, 32] and the factor $\frac{1}{2}$ is due to the fact that a secure bit exchange occurs on average 50% of the time.

The lifetime of the KLJN key, $\tau_k$, in vehicular communication networks depends on the vehicle density. For the sake of simplicity, first we assume homogenous car density:

$$n_c = \frac{N_c}{N_{KLJN}}, \tag{3}$$

where $N_c$ is the number of cars and $N_{KLJN}$ is the number of Roadside Devices with KLJN units. Thus a KLJN unit serves $n_c$ cars. Consequently the frequency of *secure* bit donation to a single car is:

$$\mathrm{f_c} = \frac{\mathrm{f_{sec}}}{n_c} \tag{4}$$

If the length of the KLJN key is defined as $N_k$, then by combining Eqs. (1)–(4), we find that the lifetime of the KLJN key in vehicular communication networks is:

$$\tau_k = \frac{N_k}{\mathrm{f_c}} = \frac{2N_k n_c \gamma L}{\Theta c} \tag{5}$$

Note that this result represents a pessimistic estimation for inhomogeneous vehicular communication networks when $n_c$ is the upper limit of the number of cars any RSD is handling. Thus, Eq. (5) gives an upper limit of the lifetime of the KLJN key in vehicular communication networks. To demonstrate the results, we assign possible practical values to the parameters. Let $L = 1000\ meters$, $c = 2 * 10^8\ meters/s$, $\gamma = 100$ (see [30,31]), $N_k = 100\ bits$, $n_c = 1000\ vehicles$, and $\Theta = 0.1$. Then the lifetime of KLJN key is $\tau_k = 10^3\ s$.

Techniques such as building parallel channels by using chip and multi-wire cables can be used to enhance the speed of the KLJN scheme and to decrease $\tau_k$ [19]. There is also a possibility to increase the security of physically exchanged keys in the case of repeated usage [33].

## 3. Conclusion

In this paper, we reviewed the communication infrastructure and discussed some security-related aspects of vehicular communication networks. We have proposed a KLJN key donation solution for vehicular communication networks. The KLJN key generation in vehicular communication networks has also been discussed and an upper limit for the lifetime of this KLJN key was computed.

**Acknowledgements**

X. Cao's contribution is supported by China Scholarship Council. Y. Saez is grateful to IFARHU/SENACYT for supporting her PhD studies at Texas A&M.

**References**

[1] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J. Hubaux, Secure vehicular communication system: design and architecture, *IEEE Commun.* **46** (2008) 100–109.

[2] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks, *Comput. Commun.* **31** (2008) 2803–2814.

[3] J. Guo, J. P. Baugh, and S. Wang, A group signature based secure and privacy-preserving vehicular communication framework, *Proc. Conf. on Mobile Networking for Vehicular Environments*, Anchorage, AKA, USA, May 2007, 103–108.

[4] K.-D., Kim and P.R., Kumar, An MPC-based approach to provable system-wide safety and liveness of autonomous ground traffic, accepted for publication on *IEEE Trans. Autom. Control* (2014), manuscript: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6882808.

[5] M. Raya, P. Papadimitratos, and J.-P. Hubaux, Securing vehicular communications, *IEEE Wireless Commun.* **13** (2006) 8–15.

[6] M. Raya and J.-P. Hubaux, The security of vehicular Ad Hoc networks, *Proc. 3rd ACM Workshop on Security of Ad Hoc Sensor Networks*, Alexandria, VA, USA, November 2005, 11–21.

[7] P. Papadimitratos, F. La, K. Evenssen, R. Bringnolo, and S. Cosenza, Vehicular communication systems: enabling technologies, applications, and future outlook on intelligent transportation, *IEEE Commun.* **47** (2009) 84–95.

[8] P. Ardelean and P. Papadimitratos, Secure and privacy-enhancing vehicular communication: Demonstration of implementation and operation, *Proc. 68th IEEE Conf. on Vehicular Technology*, Calgary, Canada, September 2008, 1–2.

[9] Y. Saez, X. Cao, L. B. Kish and G. Pesti, Securing vehicle communication systems by the KLJN key exchange protocol, *Fluct. Noise Lett*. **13** (2014) 1450020.

[10] J. Blum and A. Eskandarian, The threat of intelligent collisions, *IT Professional* **6** (2004) 24–29.

[11] M. Raya and J.P. Hubaux, Securing vehicular ad hoc networks, *Journal of Computer Security* **15** (2007) 39–68.

[12] N. Wang, Y. Huang, and W. Chen, A novel secure communication scheme in vehicular ad hoc networks*, Comput. Commun.* **31** (2008) 2827–2837.

[13] A. Studeret, E. Shi, F. Bai and A. Perrig, TACKing together efficient authentication, revocation, and privacy in VANETs, *Proc. 6th Annual Conf. on Sensor, Mesh and Ad Hoc Communications and Networks*, Rome, Italy, June 2009, 1–9.

[14] D. Boneh, X. Boyen, and H. Shacham, Short group signatures, *Proc. 24th Annual Int. Cryptology Conference*, Santa Barbara, CA, August 2004, 41–55.

[15] C. Zhang, R. Lu, X. Lin, P. Ho and X. Shen, An efficient identity-based batch verification scheme for vehicular sensor networks, *Proc. 27th Conf. on Computer Communications*, Phoenix, AZ, USA, April 2008, 13–18.

[16] C. Zhang, X. Lin, R. Lu and P. Ho, RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks, *Proc. IEEE Int. Conf. on Communications*, Beijing, CHN, May 2008, 1451–1457.

[17] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, SPECS: Secure and privacy enhancing communications schemes for VANETs, *Ad Hoc Networks* **9** (2011) 189–203.

[18] Y. Liang, H. V. Poor, and S. Shamai, Information theoretic security, *Foundations Trends Commun. Inform. Theory* **5** (2008) 355–580.

[19] L. B. Kish, Totally secure classical communication utilizing Johnson (-like) noise and Kirchoff's law*, Phys. Lett. A* **352** (2006) 178–182.

[20] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, Quantum cryptography, or unforgeable subway tokens, *Advances in Cryptology: Proceedings of Crypto '82*, Plenum Press, Santa Barbara, 1982, 267–275.

[21] R. Mingesz, L. B. Kish, Z. Gingl, C. G. Granqvist, H. Wen, F. Peper, T. Eubanks, and G. Schmera, Unconditional security by the laws of classical physics*, Metrol. Meas. Syst.* **20** (2013) 3–16.

[22] L. B. Kish, D. Abbott, and C. G. Granqvist, Critical analysis of the Bennett–Riedel attack o n secure cryptographic key distributions via the Kirchhoff-law–Johnson-noise scheme, PLo S ONE 8 (2013) e81810. Open access: http://www.plosone.org/article/info%3Adoi%2F10.1 371%2Fjournal.pone.0081810.

[23] L. B. Kish, Enhanced secure key exchange systems based on the Johnson-Noise scheme, *Metrol. Meas. Syst.***20** (2) (2013) 191–204.

[24] R. Mingesz, Z. Gingl, and L. B. Kish, Johnson (-like) -noise–Kirchhoff-loop based secure classical communicator characteristics, for ranges of two to two thousand kilometers, via model-line, *Phys. Lett. A* **372** (2008) 978–984.

[25] L. B. Kish and C. G. Granqvist, On the security of the Kirchhoff-law–Johnson-noise (KLJN) communicator, *Quantum Inf Process* **13** (2014) 2213–2219.

[26] L. B. Kish and R. Mingesz, Totally secure classical networks with multipoint telecloning (teleportation) of classical bits through loops with Johnson-like noise, *Fluct. Noise Lett.* **6** (2006) C9–C21.

[27] E. Gonzalez, L. B. Kish, and R. S. Balog, Information theoretically secure, enhanced Johns on noise based key distribution over the smart grid with switched filters, *PLoS ONE* 8 (2013) e70206. Open access: http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0070206.

[28] L. B. Kish and O. Saidi, Unconditionally secure computers, algorithms and hardware, such as memories, processors, keyboards, flash and hard drives, *Fluct. Noise Lett.* **8** (2008) L95–L98.

[29] P. Lingenfelser and P. Thilo, Loop detectors for measuring road traffic, Siemens Rev. 37 (6) (1970) 332–337.

[30] D. Middleton, H. Charara, and R. Longmire, Alternative vehicle detection technologies for traffic signal systems: technical report, *Research Report FHWA/TX-09/0-5845-1*, Texas Transportation Institute, The Texas A&M University System, College Station, TX, February 2009.

[31]Y. Saez, L. B. Kish, Errors and their mitigation at the Kirchhoff-Law-Johnson-Noise secure key exchange, *PLoS ONE* **8** (2013) e81103. Open access: http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0081103.

[32] Y. Saez, L. B. Kish, R. Mingesz, Z. Gingl, and C. G. Granqvist, Current and voltage based bit errors and their combined mitigation for the Kirchhoff-law–Johnson-noise secure key exchange, *J. Comput. Electron*. 13 (2014) 271–277.

[33] L. B. Kish, Enhanced usage of keys obtained by physical, unconditionally secure distributions, manuscript http://arxiv.org/abs/1408.5800 (2014), version 1.