

Authentic Batteries: A Concept for a Battery Pass Based on PUF-enabled Certificates

Julian Blümke

C-ECOS

Technische Hochschule Ingolstadt

Ingolstadt, Germany

e-mail: julian.bluemke@carissma.eu

Hans-Joachim Hof

C-ECOS

Technische Hochschule Ingolstadt

Ingolstadt, Germany

e-mail: hof@thi.de

Abstract—The European Union’s Green Deal and other similar regulations advocate to reuse batteries of electrical vehicles (“second life”) to reduce greenhouse gases. To ease the assessment of the best fitting second life applications for a distinctly used battery, product life cycle data plays an important role. A digital battery pass will be mandatory for future batteries and will contain such data collected throughout the product’s life cycle. Having trustworthy data is one key element of the battery pass in order to provide authentic batteries. This paper presents a concept to securely bind the pass to the battery itself by using physical unclonable functions for creating a unique identifier per battery. The approach is based on certificates and makes use of Certificate Transparency to foster trust in the issued certificates. Attacks on product life cycle data or certificates and counterfeiting batteries can be detected.

Index Terms—*physical unclonable function; Certificate Transparency; electric vehicle battery; battery identity; battery pass.*

I. INTRODUCTION

The European Union’s (EU) Green Deal aims to reduce greenhouse gases towards net-zero emissions by 2050 [1]. One of the measures is to lower the use of fossil energies in the transportation sector. Electrically driven vehicles foster this goal and are expected to achieve high sales numbers in the upcoming years: The Faraday Institute forecasts a worldwide demand of more than 5,900 GWh in the year 2040 (2020: 110 GWh) [2]. The rise of Electrical Vehicles (EV) is accompanied by an increasing need for high voltage batteries. However, batteries degrade during usage and charging. They can only be used in an EV until their capacity degraded to 80% [3] [4]. This will result in a large number of dismantled and unusable EV-batteries having a negative economical, ecological and social impact [5]–[7]. However, these batteries may be still fine for other use cases. To support recycling and reusing of products and materials the EU introduced the Circular Economy Action Plan containing the reuse of batteries as one pillar [8]. Its goal is to set up applications for a battery’s second life either as complete product in a different environment or dismantled in new products.

The new mass market for EV batteries will also encourage the production of counterfeit batteries. Non-certified or non-qualified batteries can introduce safety risks due to deviations from specifications of genuine products and especially due to cost-savings in risk reducing controls and management sys-

tems [9]. Reduced capacity and lifetime, overheating, and self-ignition, as well as social aspects like underpaid workers and bad working conditions during manufacturing are examples for likely effects when using counterfeit EV-batteries.

Circular economy and the fight against counterfeiting emphasize a need for authentic batteries: Trust in the battery’s quality, evidence in the correct implementation of the specification, and traceability of the product life cycle enhance the opportunities for second life applications and lower the risk of introducing low quality and dangerous products into the market.

Both, the readiness for circular economy and the circulation of only high-quality batteries, shall be regulated within the new and as of today drafted EU-regulation about the treatment of (old) batteries [10]. The proposal presents a digital battery pass as a record of manufacturer, materials, and specifications of every single battery. This paper presents an approach to inherently bind the digital pass to the physical battery by using certificates based on Physical Unclonable Functions (PUF).

Physical Unclonable Function: A PUF uses physical deviations that occur during production to create a unique and unclonable identifier [11]. It is described as a challenge-response-pair (CRP) where a device to be authenticated needs to prove the ownership of the PUF-identifier. There are two different types: weak PUFs always provide the same identifier, strong PUFs can create multiple identifier. An example for a weak PUF is the SRAM-PUF which takes advantage of the cells’ random behavior after powering whereas an optical PUF where randomly distributed particles on a surface are illuminated from different directions creating unique shadows is an example for a strong PUF [12]. PUFs are used as an computational and financial inexpensive alternative of storing cryptographic keys or identifier in non-volatile memory [11].

Certificate Transparency: Certificate Transparency (CT) was originally developed by Google and is about transparent and trust-worthy issuing of certificates used in the Web PKI [13]. It is summarized in the experimental RFC 6962 [14] and deals with the difficulties of trusting Certificate Authorities (CA) in general: private keys associated with a certificate may be stolen or created in a wrongful way such that encryption

itself would not be damaged but an attacker might be able to decrypt the communication without knowledge of the necessary key. A common way to check the trustworthiness of CAs is to examine audits. However, audits often check for formal aspects only than for a correct implementation of technical processes.

The idea of CT is about storing certificates in publicly available append-only logs that can be validated by everyone. Figure 1 shows the steps needed to implement CT: The owner of the domain requests a certificate by the CA which creates a pre-certificate and sends it to the log. The latter is managed as a Merkle Tree [15]. A Signed Certificate Timestamp (SCT) ensuring that the certificate is added to the log is send to the CA. The certificate is extended with the SCT and transferred the domain owner. From this time on, the domain owner can use it as normal certificate, e.g., for hosting websites. At the end user's site, the certificate is checked for the existence of SCTs, e.g., during TLS handshake. Some internet browser require that the certificate is signed with at least two SCTs. The certificate logs are checked periodically by external monitors. The domain owner is informed if there are new and especially odd activities with certificates of its domain.

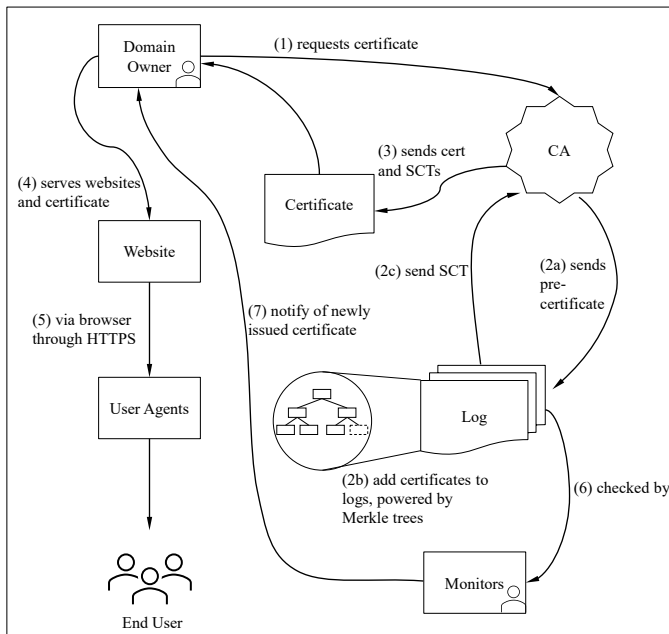


Fig. 1. Implementation of certification transparency (illustration based on [13]).

Furthermore, there are other methods for detecting counterfeit products, e.g., by statistical measures [16], physical inspection, or electrical examination [17]. However, the presented concept is triggered by the EU regulation concerning the battery pass and therefore, the concept of logging and auditing is reasonable.

The remaining paper is structured as followed: Section II describes related work as a basis for a concept for authentic

batteries which is introduced in Section III. Current and future activities are summarized in Section IV.

II. RELATED WORK

To the best of our knowledge, the idea of a digital product pass for single products is unique to batteries. Other applications do have static product records or they are only implemented for a group of products and not for single devices, e.g., like the International Material Data System (IMDS) [18], the Building Information Modeling (BIM) based Material Passport [19], or the Cradle-to-Cradle (C2C) Passport [20]. Additionally, the battery pass will be the first pass that is required by law. The following related research results introduce only comparable parts of the presented concept.

A. PUFs based on batteries

In [21], Bosch describes the calculation of PUF identifiers out of a set of different parameters: pressure drop between two sides of the battery, the batteries natural frequency, the temperature pattern, the open circuit voltage (OCV) or the air leak rate [21]. The created PUF identifier is saved as a physical tag on top of the battery or in the battery management system's memory. However, the identifier can only be calculated in a dismantled state. This method shows the possibility of a battery PUF creation in general.

[22] presented a method to authenticate an outstation in a distributed energy storage network. This work takes advantage of the fact that the cells' voltages differ at the same state of charge (SoC). Both, the outstation and the master station, sanitize a challenge-reply-table with continuously updated measurements presenting a model of every cell. The authentication challenge is formed out of a selection of cells. The SoC and the voltages are measured and sent back to the master station. If the actual measurements match with the values in the challenge-reply-table the outstation is accepted as authentic.

Both works demonstrate that it is feasible to use PUFs on batteries. However, existing works use the PUF as a mechanism to create an identity. We want to extend this to use the PUF as a derivation for cryptographic keys.

B. Blockchain with PUFs

A common mechanism to implement digital product passes is the use of blockchain [23] [24]. Casino et al. described a blockchain as "distributed append-only timestamped data structure" [25] where no central and trusted authority is involved. Exchanging assets, digital or physical, between two blockchain participants is achieved and recorded with transactions. They have to be validated by other participating nodes using a consensus algorithm in order to prevent corruption or forgery of branches. Blockchains in the sector of supply chain management can increase trust, traceability, transparency and accountability. They are installed for better visibility and enhanced optimization of a supply chain. [25]

PUFChain is a method that combines blockchain with PUFs within the Internet-of-Everything (IoE) domain where trusted

nodes authenticate IoE-data collected from client nodes [26]. The process is divided in three phases: During the enrollment, the client's PUF-CRP are calculated and stored in a secure database. The phases of transactions consist of data collection, PUF response generation, and hashing of both. The data and the hash is added to the blockchain and needs to be authenticated by trusted nodes. These nodes recalculate the hash by using the client data and the pre-calculated PUF response retrieved from the database and validate the block if both hashes match. An application of PUFChain in the Internet-of-Energy can be found in [27].

An approach to enable trust in supply chain by tracing was presented in [28]. Newly manufactured devices need to be registered in a blockchain with a unique ID, e.g., a PUF. Device transfers are recorded in the blockchain. The contractual ownership alters only after a transfer confirmation which is done by calculating the unique device ID of the received device and comparing it with the ID mentioned in the transaction payload. End users can check the device's authenticity by matching the computed ID with the blockchain content.

Whereas blockchain is a popular method for storing tamper-proofed data, we decided to use a different approach. In our opinion, the system consists for trusted partners. Therefore, a decentralized distribution of data is not necessary. A database can be hosted, e.g., by the EU enforcing the battery regulations. Another aspect is that in this specific application consensus algorithms are useful only to a limit extent as it will just provide a proof of formal attributes of transaction but not on the transaction content itself: For example a blockchain party validating a new block cannot check the correctness of, e.g., a new temperature maximum or a degradation of capacity as it does not have access to the battery itself.

III. CONCEPT FOR AUTHENTIC BATTERIES

A. Introduction

The general aim of our method is to have one single source of truth containing information about the battery's life cycle including the manufacturing process, product acceptance tests (PAT), measures of quality control, and the usage history. Tracing materials and processes foster consumer's trust in the battery and enables an easier assessment of the batteries' status for recycling or reusing.

The data of the life cycle record is stored in a database that can be permissioned in order to control and restrict read and write access of supply chain parties involved. Access control also protects the parties' intellectual property (IP). It is mandatory to have a secure binding between the life cycle record and the battery itself ensuring the correspondence between both. The secure binding is established by the use of certificates in combination with PUFs that provide unique identifiers for each battery.

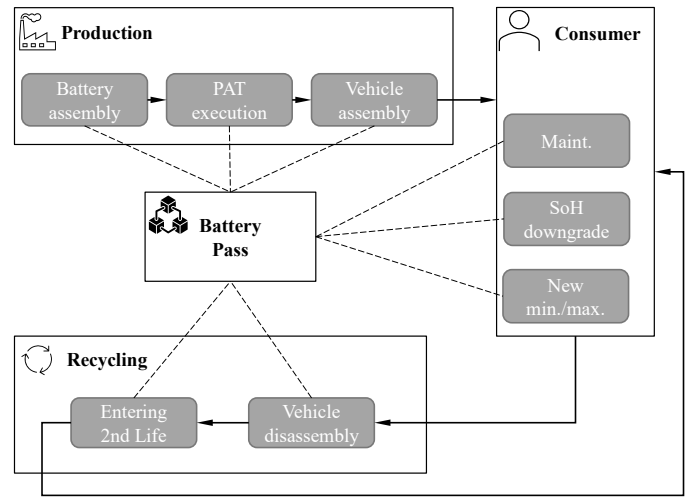


Fig. 2. Battery pass as life cycle record.

B. Data for battery pass's records

Data is added to the battery pass during manufacturing, product testing, and quality controlling. At end user level, the data is needed to emphasize a remarkable downgrade of, e.g., the state of health (SoH) or capacity and to record minimum and maximum temperatures, voltages and currents. The latter are important to assess the batteries health for a second life application. The data acquisition building the life cycle record is split into three phases (see Figure 2).

Assembly and initial product testing takes place during the production stage at the battery OEM (original equipment manufacturer). Information about manufacturer, working conditions, date of production, and results of acceptance tests are stored in the battery pass. Afterwards, the battery is transferred to the vehicle's OEM to be built into the intended vehicle. Again, information about the vehicle manufacturer, working conditions, and the vehicle including the vehicle identification number (VIN) are stored in the record.

We are assuming the car to be delivered to the consumer directly after production. At this stage the battery will be used in its intended environment. Significant changes of the battery's quality will be logged to the life cycle record. These changes include temperature, voltage and current maxima and minima and SoH and capacity downgrade. This information will ease the battery's assessment before entering the second life.

The preparation of the second life is divided into two steps: First, the battery is dismantled from the vehicle and the date and the implementing company are stored in the life cycle record. The activity of entering the second life contains events like firmware updates, quality tests and maintenance activities. Again, the battery will be transferred to a consumer. We assume an environment in which the life cycle record can be sanitized. Therefore, the stage of the second life equals the consumer stage.

The format of the battery pass's data is not defined inhere.

However, the JSON data format may be reasonable as it is widely used and easy to read and process.

C. Security Considerations

With the presented concept the following security related aspects shall be considered: The battery pass and its records shall be bound to the battery in order to state out that these records are only valid for this specific battery. Manipulation of the battery pass has to be detectable as well as the circulation of counterfeit batteries having no or stolen battery passes. Updates of the records shall only be possible from the battery itself or from a system that has access to the battery. This ensures the validity of the data without the possibility of data added by a third-party not involved in the process. Trust and transparency shall be treated to foster the battery pass's acceptance by the user and in general a successful assessment of second life applications.

D. Security Architecture

The technical implementation of our method is based on signed battery data whereas the keys are derived from the battery's PUF. Figure 3 shows the overall process of adding data and verifying the battery's identity. We are assuming the private and public key derived from the PUF already exist. As elaborated in the related work section (Section II), this is a reasonable assumption.

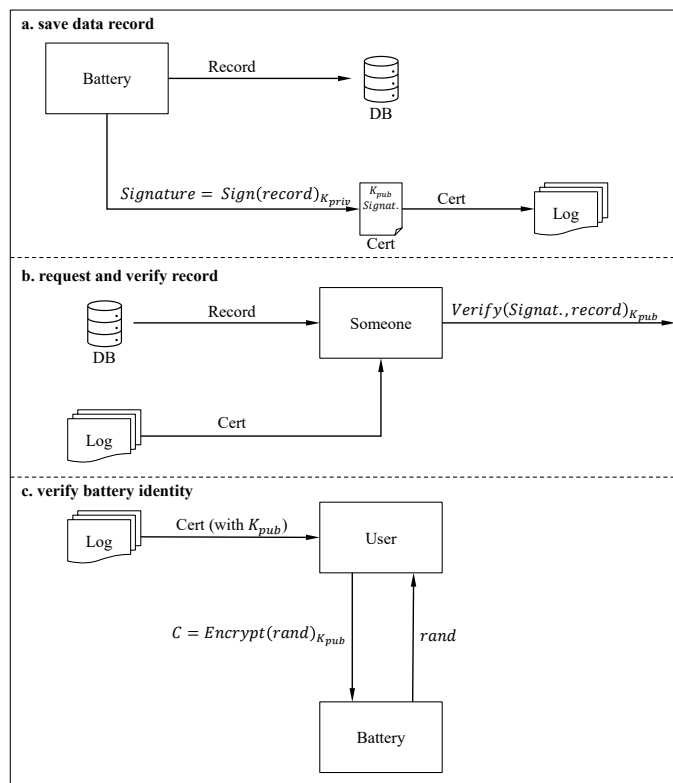


Fig. 3. Implementation of digital pass with certificates. **a.** Update of battery records **b.** Verify that certificate belongs to records **c.** Verify that battery belongs to certificate.

Three phases are applicable:

The most functional part of the method is adding and updating data of the battery as it is described in Sec. III-B. If new data is generated it will be sent to a central database containing historic and current data of each battery (Figure 3a). In the battery the data is signed with its private key. Only the signature is added to a battery specific certificate also containing the public key. If a certificate already exists for the battery a reissuing is needed and the old one has to be revoked. The certificate itself is attached to an append-only log. We are relying on Certificate Transparency which is a commonly used method developed by Google to store and handle identity certificates in a trusted and verifiable way. Whereas the log itself does not fulfill any functional requirement, it provides additional trust and transparency into the certificate as it can be validated from external and public parties.

One could argue to add the battery data to the certificate introducing the advantage of having one single document containing all relevant information about the battery. However, having this, the battery's data is publicly available and therefore, IP may be revealed as well as the opportunity for malicious analysis about production statistics and performance of a battery OEM. A dedicated database can be restricted to a reduced number of users.

In order to check the validity of the data in accordance with the corresponding certificate, access to the data and the certificate is needed. Using the public key stored in the certificate the signatures can be verified (Figure 3b). In this context, another opportunity to avoid disclosure of IP may be possible by letting the signatures be checked by the database itself and letting it deliver a summary of data not revealing IP.

In the third phase, it is checked that the certificate belongs to the battery as described in Figure 3c. Therefore, a challenge-response-mechanism is used where the user sends a challenge consisting of random number encrypted with the public key to the battery. The challenge is decrypted using the battery's private key and the response is sent back to the user. If the response equals the original random number it is verified that the certificate belongs to the battery as the private key is directly derived from the battery's PUF.

To reduce the risk of stolen or reproduced keys by an attacker the derived key may be stored in a Hardware Security Module (HSM), e.g., placed on the Battery Management System (BMS). However, the cost-efficiency of HSMs in the context of industrial applications with large quantities having high pressure on costs has to be evaluated [29].

E. Challenges

The main challenge of the presented method is the derivation of keys from the battery's PUF. It is required that the keys do not change over time. However, due to aging of cells and the battery pack the PUF and therefore, the keys may change. The validation steps mentioned above cannot be executed anymore resulting in a failure of the complete method. The same applies

for genuine repairs or maintenance activities of the battery. Single cells will not be exchanged probably, but battery packs. This would result in a new PUF and so in invalid existing private and public keys.

To overcome both, two approaches might be appropriate: First, using a model forecasting the cell and battery aging in order to create static cryptographic keys. And second, if an imminent change is foreseeable having a mechanism to modify the existing keys, e.g., with pre-calculated challenges and a hash chain for tracking expired keys.

Instead of using the battery's cells to create unique identifier one could also use the surrounding electrical components as origin for physical unclonable functions. The entropy might be enough to create cryptographic keys as there are many components built in one battery pack. These components do not age in the same way as cells do.

Challenges also arise in the general use of the battery pass. Standardization across companies is mandatory to enable comparability of batteries. This also applies for the update procedure of the battery pass. Questions concerning the frequency and the resolution of record updates have to be answered.

F. Security Analysis

In the following section it is analyzed if the presented concept complies with the requirements stated in Section III-C.

Attack Model: We assume that the attacker has read and write access to the database. As the certificates are stored publicly following the methods of Certificate Transparency the adversary can read certificates. However, the attacker cannot read or re-create the battery's private key as we assume that the physical access to the battery and its related components is restricted.

Binding battery pass and battery: The battery pass and the physical battery are bound using the cryptographic keys created from the battery's PUF.

Detection of manipulated battery pass: A manipulation of data in the database will be recognized when the data's signature is verified. The verification of the signatures should be a mandatory step when working with these batteries, e.g., for an assessment of the second life applications.

However, manipulation or deletion of data can result in financial and ecological damage as it is the basis for further use of the battery. If the data is deleted, assumptions based on statistical measures have to be consulted which may result in a worse assessment of the state of health.

Circulation of counterfeit batteries: If an attacker duplicates the certificate in order to sell a counterfeit battery with a pseudo-valid certificate, the attack may not be recognized until the link between the certificate and the battery is verified. Whereas signature for the data is valid, the challenge-response will fail: The public key of the certificate does not match to the private key of the battery. Therefore, the decryption of the response will fail.

Update of battery pass only with access to battery: Records can be added to the database without having access to the battery. However, the battery pass, i.e., the certificate can only be reissued with the record's signature which is created with the cryptographic keys derived from the PUF. Therefore, a valid update of the battery pass is only possible with physical access to the battery.

Generating trust and transparency: Trust and transparency for user's acceptance and for trustworthy assessment of second life applications is created with the use of cryptographic keys on the one hand and on the other hand with the use of Certificate Transparency where certificates can be validated by external parties.

Several attack scenarios have been described. None of them can be executed on its own as there need to be attacks on multiple system parts to be successful. However, it also showed that a verification of the different links between certificate, data and battery is mandatory to ensure the system's security.

Nevertheless, a complete and in-depth security analysis will be executed in the future to strengthen the given statements.

G. Efficiency of Data Transfer and Verification

In the current EU project MARBEL (Manufacturing and assembly of modular and reusable Electric Vehicle battery for environment-friendly and lightweight mobility) the efficiency of data transfer with a state-of-the-art BMS has been analyzed in a Proof-of-Concept. Tests have been made with a frequency of data transfer ranging from 5 Hz to 200 Hz sending single MQTT (Message Queuing Telemetry Transport protocol) messages. Authentication and encryption was established using the Transport Layer Security (TLS) protocol adding a security related overhead to every message. The average message size summed up to 90 bytes which corresponded to a measured maximum data rate of 144 kBits/s. The findings from these tests appear to support the assumption of an efficient data transfer. However, a continuous stream of battery data might not be required as the degradation of the battery's state of health is a slow process. Data may be also buffered over a defined time and sent in blocks.

Data will be verified on servers which can be highly optimized. Therefore, it is expected that the verification can be carried out efficiently as well.

IV. CONCLUSION AND FUTURE WORK

Circular economy and the fight against product counterfeiting increase the need for authentic products. The digital battery pass is one example for achieving trust and traceability of a product. The paper presented a concept to manage a battery's life cycle record by using certificates. The correspondence between the batteries identity and the battery pass is achieved with PUFs constructed of the battery's physical deviations. Using the PUF-enabled certificates, it is possible to detect counterfeit as well as low-quality batteries. Challenges occur in the consistency of PUFs due to aging and maintenance

issues of the product pass.

Future work includes the implementation of a Proof-of-Concept followed by a performance analysis and an in-depth formal security analysis in order to evaluate the functionality in general and the security measures of the concept. Other mechanisms for detecting counterfeit electronic products will be analyzed and might enhance the presented concept. The consistency of PUFs in the context of batteries will be part of further extensive investigations.

ACKNOWLEDGMENT

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 963540.



I want to thank my research colleagues for supporting me during the concept creation. I also want to acknowledge the research group of Prof. Dr. rer. nat. Hans-Georg Schweiger for discussions about the topic of PUFs for batteries.

REFERENCES

- [1] European Commission, "Regulation (eu) 2021/1119 of the european parliament and of the council of 30 june 2021 establishing the framework for achieving climate neutrality and amending regulations (ec) no 401/2009 and (eu) 2018/1999 ('european climate law'): European climate law," 2021. [Online]. Available: <http://data.europa.eu/eli/reg/2021/1119/oj>
- [2] "Lithium, cobalt and nickel: The gold rush of the 21st century." [Online]. Available: <https://faraday.ac.uk/get/insight-6/>
- [3] E. Wood, M. Alexander, and T. H. Bradley, "Investigation of battery end-of-life conditions for plug-in hybrid electric vehicles," *Journal of Power Sources*, vol. 196, no. 11, pp. 5147–5154, 2011.
- [4] E. Hossain, D. Murtaugh, J. Mody, H. M. R. Faruque, M. S. Haque Sunny, and N. Mohammad, "A comprehensive review on second-life batteries: Current state, manufacturing considerations, applications, impacts, barriers & potential solutions, business strategies, and policies," *IEEE Access*, vol. 7, pp. 73 215–73 252, 2019.
- [5] L. A.-W. Ellingsen, G. Majeau-Bettez, B. Singh, A. K. Srivastava, L. O. Valøen, and A. H. Strømman, "Life cycle assessment of a lithium-ion battery vehicle pack," *Journal of Industrial Ecology*, vol. 18, no. 1, pp. 113–124, 2014.
- [6] J. F. Peters, M. Baumann, B. Zimmermann, J. Braun, and M. Weil, "The environmental impact of li-ion batteries and the role of key parameters – a review," *Renewable and Sustainable Energy Reviews*, vol. 67, pp. 491–506, 2017.
- [7] C. Thies, K. Kieckhäfer, T. S. Spengler, and M. S. Sodhi, "Assessment of social sustainability hotspots in the supply chain of lithium-ion batteries," *Procedia CIRP*, vol. 80, pp. 292–297, 2019.
- [8] European Commission and Directorate-General for Communication, *Circular economy action plan: for a cleaner and more competitive Europe*. Publications Office, 2020.
- [9] A. B. Lopez, K. Vatanparvar, A. P. Deb Nath, S. Yang, S. Bhunia, and M. A. Al Faruque, "A security perspective on battery systems of the internet of things," *Journal of Hardware and Systems Security*, vol. 1, no. 2, pp. 188–199, 2017.
- [10] European Commission, "Proposal for a regulation of the european parliament and of the council concerning batteries and waste batteries, repealing directive 2006/66/ec and amending regulation (eu) no 2019/1020," 17.03.2022. [Online]. Available: <http://data.consilium.europa.eu/doc/document/ST-7317-2022-INIT/X/pdf>
- [11] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proceedings of the 44th annual Design Automation Conference*, ser. ACM Conferences, S. P. Levitan, Ed. New York, NY: ACM, 2007, p. 9.
- [12] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A puf taxonomy," *Applied Physics Reviews*, vol. 6, no. 1, p. 011303, 2019.
- [13] Google, "Certificate transparency: How it works," 2022. [Online]. Available: <https://certificate.transparency.dev/howitworks/>
- [14] B. Laurie, A. Langley, and E. Kasper, "Certificate transparency," 2013. [Online]. Available: <https://www.rfc-editor.org/info/rfc6962>
- [15] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Advances in Cryptology — CRYPTO '87*, C. Pomerance, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1988, pp. 369–378.
- [16] K. Huang, Y. Liu, N. Korolija, J. M. Carulli, and Y. Makris, "Recycled ic detection based on statistical methods," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 6, pp. 947–960, 2015.
- [17] U. Guin, K. Huang, D. Dimase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1207–1228, 2014.
- [18] F. B. de Oliveira, A. Nordelöf, B. A. Sandén, A. Widerberg, and A.-M. Tillman, "Exploring automotive supplier data in life cycle assessment – precision versus workload," *Transportation Research Part D: Transport and Environment*, vol. 105, p. 103247, 2022.
- [19] M. Honic, I. Kovacic, P. Aschenbrenner, and A. Ragossnig, "Material passports for the end-of-life stage of buildings: Challenges and potentials," *Journal of Cleaner Production*, vol. 319, p. 128702, 2021.
- [20] T. Adisorn, L. Tholen, and T. Götz, "Towards a digital product passport fit for contributing to a circular economy," *Energies*, vol. 14, no. 8, p. 2289, 2021.
- [21] K. Vittilapuram Subramanian and A. Madhukar Lele, "A system and method for generation and validation of puf identifier of a battery pack," Patent WO2022023280A2, 2022.
- [22] I. Zografopoulos and C. Konstantinou, "Derauth: A battery-based authentication scheme for distributed energy resources," in *2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, 2020, pp. 560–567.
- [23] M. Kouhizadeh, J. Sarkis, and Q. Zhu, "At the nexus of blockchain technology, the circular economy, and product deletion," *Applied Sciences*, vol. 9, no. 8, p. 1712, 2019.
- [24] T. K. Agrawal, V. Kumar, R. Pal, L. Wang, and Y. Chen, "Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry," *Computers & Industrial Engineering*, vol. 154, p. 107130, 2021.
- [25] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55–81, 2019.
- [26] S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "Pufchain: A hardware-assisted blockchain for sustainable simultaneous device and data security in the internet of everything (ioe)," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 8–16, 2020.
- [27] R. Asif, K. Ghanem, and J. Irvine, "Proof-of-puf enabled blockchain: Concurrent data and device security for internet-of-energy," *Sensors (Basel, Switzerland)*, vol. 21, no. 1, 2020.
- [28] P. Cui, J. Dixon, U. Guin, and D. Dimase, "A blockchain-based framework for supply chain provenance," *IEEE Access*, vol. 7, pp. 157 113–157 125, 2019.
- [29] Y. Xie, Y. Guo, S. Yang, J. Zhou, and X. Chen, "Security-related hardware cost optimization for can fd-based automotive cyber-physical systems," *Sensors (Basel, Switzerland)*, vol. 21, no. 20, 2021.