Demo: Certificateless and Non-Interactive Key Establishment for Secure CCS EV Charging

Muhammad Jahanzeb Khan, Hassan Mahmoud, Dylan Canipe, Mahmoud Nabil Mahmoud, Mizanur Rahman, Ahmad Alsharif
The University of Alabama

Abstract

We demonstrate a certificateless, non-interactive key establishment mechanism integrated into the SLAC pairing process for CCS-based EV charging. The proposed integration leverages identity-based cryptography to replace plaintext NMK delivery with a decentralized non-interactive key derivation, eliminating additional message exchanges and certificate overhead. Compared to ECDH-based approaches, our method avoids interactive key exchange and reduces man-in-the-middle exposure at the PLC layer by eliminating plaintext NMK delivery. When combined with policy-controlled fallback, the design also reduces downgrade opportunities during SLAC key establishment. Our integration is implemented and verified on HomePlug Green PHY (HPGP) testbeds using ISO 15118-3 SLAC, preserving compatibility with the standard SLAC procedure and avoiding PKI overhead.

1 Introduction

The Combined Charging System (CCS) is the dominant standard for DC fast charging in Electric Vehicles (EVs). CCS relies on ISO 15118, which establishes communication between the EV and Electric Vehicle Supply Equipment (EVSE) over Power Line Communication (PLC). ISO 15118-3 defines the physical- and link-layer behavior of this link. During the connection phase, the Signal Level Attenuation Characterization (SLAC) mechanism performs an attenuation-based matching procedure to verify pairing between the two endpoints. Once pairing succeeds, the EVSE provisions the Network Membership Key (NMK) that secures PLC communication. However, the NMK is transmitted in plaintext, and prior work shows that an adversary can exploit electromagnetic leakage to capture it, enabling unauthorized traffic decryption [1].

To address this vulnerability, prior work proposed integrating an Elliptic Curve Diffie-Hellman (ECDH) key exchange into SLAC [1]. While this prevents plaintext NMK disclosure, it introduces additional message exchanges and lacks inherent authentication, leaving the protocol vulnerable to man-in-the-middle attacks [2]. Mitigation requires a certificate-based Public Key Infrastructure (PKI), which adds complexity in large-scale deployments due to certificate issuance, distribution, and validation. Furthermore, studies show that CCS deployments support insecure fallback modes, enabling downgrade attacks against version negotiation and optional TLS [3, 4].

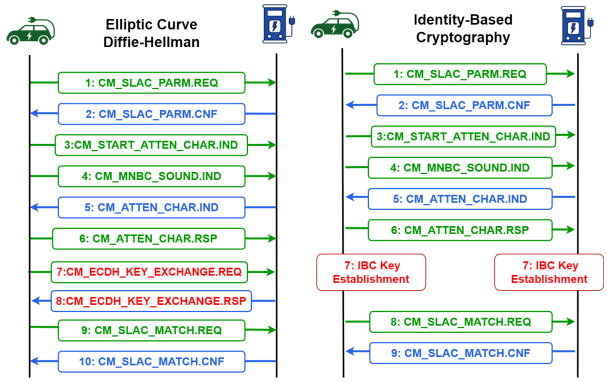


Figure 1: SLAC Protocol with ECDH VS IBC

In this work, we integrate a decentralized, non-interactive Identity-Based Cryptography (IBC) key establishment mechanism into SLAC. As shown in Figure 1, the ECDH-based design requires an additional key-exchange phase and certificate-based validation. In contrast, the proposed IBC approach allows both entities to derive a shared NMK locally from their identities and manufacturer-issued private keys. This certificateless design eliminates per-session certificate management and plaintext key exposure. Since both parties locally derive the NMK, the design removes the plaintext key-delivery step that enables PLC-layer attacks; however, downgrade resistance in mixed deployments requires authenticated capability negotiation or operator policy that disables insecure fallback.

2 Non-Interactive Key Establishment

We adopt the multi-PKG IBC model of Wang [5], in which each EV and EVSE manufacturer operates an independent Private Key Generator (PKG), denoted M_{EV} and M_{EVSE}. Public



Figure 2: CCS PLC testbed using HPGP boards.

parameters of each PKG are distributed to all parties through an authenticated out-of-band channel, e.g., embedded at production or via firmware updates. This model assumes that manufacturers or charging-network authorities securely provision device private keys and maintain the identity lifecycle, including revocation and re-keying when devices or PKG credentials are compromised.

Initialization. Let $\mathbb{G}_1$ be an additive cyclic group of prime order q with generator P, $\mathbb{G}_2$ a multiplicative cyclic group of the same order, $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ a bilinear pairing, and $H : \{0,1\}^* \to \mathbb{G}_1$ a cryptographic hash function. The EV manufacturer chooses a master secret $s_{\mathsf{M_{EV}}} \in \mathbb{Z}_q^*$ and publishes $\mathsf{mpk}_{\mathsf{M_{EV}}} = s_{\mathsf{M_{EV}}} P$. For an EV with identity $\mathrm{ID}_{\mathrm{EV}}$ (e.g., its MAC address), the public and private keys are:

$$Q_{\mathrm{EV}} = H(\mathrm{ID}_{\mathrm{EV}} \parallel \mathsf{M_{EV}}), \qquad SK_{\mathrm{EV}} = s_{\mathsf{M_{EV}}} \cdot Q_{\mathrm{EV}}$$

where Q_{EV} is publicly computable while SK_{EV} is provisioned by $\mathsf{M_{EV}}$. The EVSE keys Q_{EVSE} and SK_{EVSE} are derived analogously under $\mathsf{M_{EVSE}}$.

Shared-key derivation. Using the keys above, the EV and EVSE compute, respectively:

$$K_{\mathrm{EV}} = \hat{e}(SK_{\mathrm{EV}}, Q_{\mathrm{EVSE}}) \cdot \hat{e}(Q_{\mathrm{EV}}, \mathsf{mpk}_{\mathsf{M_{EVSE}}})$$
$$K_{\mathrm{EVSE}} = \hat{e}(Q_{\mathrm{EV}}, SK_{\mathrm{EVSE}}) \cdot \hat{e}(\mathsf{mpk}_{\mathsf{M_{EV}}}, Q_{\mathrm{EVSE}})$$

By the bilinearity of $\hat{e}$, both reduce to the same shared key:

$$K = \hat{e}(Q_{\mathrm{EV}}, Q_{\mathrm{EVSE}})^{s_{\mathsf{M_{EV}}} + s_{\mathsf{M_{EVSE}}}}$$

The derivation runs locally before SLAC matching and adds no messages to the protocol.

3 Testbed Implementation and Demonstration

The scheme was implemented on a CCS PLC testbed[1] using two devolo dLAN Green PHY Eval Board II devices, each integrating a Qualcomm QCA7000 HPGP modem and an

[1] https://github.com/jahanxb/noninteractive-ibc-slac.git

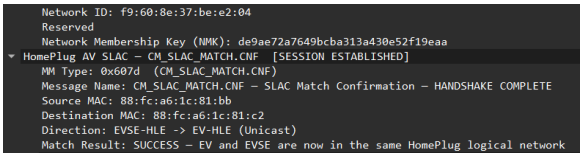


Figure 3: Captured `CM_SLAC_MATCH.CNF` message showing successful derivation of non-interactive IBC-based NMK.

NXP LPC1758 microcontroller. The boards were configured as EV and EVSE nodes (Figure 2), connected via their J3 PLC interfaces using a copper cable to emulate the charging channel, and interfaced with Ubuntu hosts for control and packet capture. The boards' MAC addresses serve as identities.

The ISO 15118-3 SLAC implementation was extended to incorporate the proposed IBC-based key establishment, replacing the plaintext NMK exchange with local derivation at both nodes without introducing additional key-exchange frames. Traffic was monitored using Wireshark/`tshark` with the HomePlug AV EtherType filter (`0x88E1`). Successful execution was confirmed when the EV transmitted `CM_SLAC_MATCH.REQ` and the EVSE responded with `CM_SLAC_MATCH.CNF`. As shown in Figure 3, both nodes derived an identical NMK across all trials.

Acknowledgments

This work was supported by Alabama Transportation Institute and the National Center for Transportation Cybersecurity and Resiliency. The views expressed are those of the authors.

References

[1] R. Baker and I. Martinovic, "Losing the car keys: Wireless PHY-Layer insecurity in EV charging," in *28th USENIX Security Symposium*, pp. 407–424, 2019.

[2] L. Eder, J. Löw, and H.-J. Hof, "Charging communication sniffing and man-in-the-middle attacks," in *Proceedings of the 16th ACM International Conference on Future and Sustainable Energy Systems*, pp. 799–804, 2025.

[3] M. Zhdanova *et al.*, "Local power grids at risk–an experimental and simulation-based analysis of attacks on vehicle-to-grid communication," in *Proceedings of the 38th Annual Computer Security Applications Conference*, pp. 42–55, 2022.

[4] M. Szakály, S. Köhler, and I. Martinovic, "Current affairs: A security measurement study of CCS EV charging deployments," in *34th USENIX Security Symposium*, pp. 7997–8015, 2025.

[5] S. Wang and Z. Cao, "Practical identity-based encryption (IBE) in multiple PKG environments and its applications." Cryptology ePrint Archive, Paper 2007/100, 2007.