Efficient Scheme for Secure and Privacy-Preserving Electric Vehicle Dynamic Charging System

Authors: Surya Teja Gunukula, Dr. Mohammed Mahmoud; Department of Electrical And Computer Engineering

1. ABSTRACT

The dynamic charging technology will enable Electric Vehicles (EVs) to charge their batteries while moving. In order to provide secure and efficient charging services to EV the dynamic charging system should allow only authorized EVs to access the system and should ensure the payment integrity. In this paper, we propose an efficient scheme to secure the dynamic charging system and to preserve the privacy of the drivers. The scheme uses a combination of different cryptosystems to achieve security and privacy. Anonymous coins are used to ensure anonymous payment and authentication. Our analysis demonstrates that the proposed scheme is secure and can preserve privacy. In addition, our measurements confirm that the proposed scheme is efficient.

2. INTRODUCTION

- Electric vehicle (EV) is a vehicle that does not use any gasoline as source of energy. Instead, it is driven by an electric motor that uses a stored battery to provide electricity. It is a form of green transportation.
- However, one of the major challenges of EV deployment is the large time needed to charge battery and the maximum driving range.
- ***Dynamic charging*** is a promising technology that can address this issue by enabling the EVs to charge while moving.
- In dynamic charging systems, charging pads are placed under a portion of roadbed and an EV's battery is charged when the vehicle drives over the pads by using electromagnetic induction [1].
- The dynamic charging system should communicate with the EVs to only charge the authorized vehicles and ensure payment integrity.
- However, this communication should be secured to avoid stealing energy by charging EVs without payment. Also, this communication should not leak sensitive information of EV drivers, especially location information.
- We mainly focus on the security and privacy issues, namely the authentication and traceability problem.

3. PROBLEM DESCRIPTION

- The proposed scheme should consider the characteristics of dynamic charging system
  - •Large number of charging pads [4]
  - •Limited computational resources
  - •Short Contact time between pads and EV
- So, by considering the above mentioned limitations the proposed scheme should use light weight cryptography to achieve fast authentication and some efficient cryptography tools to protect the privacy of users.

4. NETWORK MODEL

- As illustrated in Fig. 1, the considered network model has a bank, a charging station, and EVs. Each charging station has a charging station provider (CSP), road side units (RSUs), and Charging Pads.
- For the threat model, we focus on two main types of attacks against driver privacy and the payment. Attackers can be both internal and external.
- We have designed our network model in hierarchical architecture, so that we can easily manage the secret keys distribution among all the entities in the dynamic charging system.

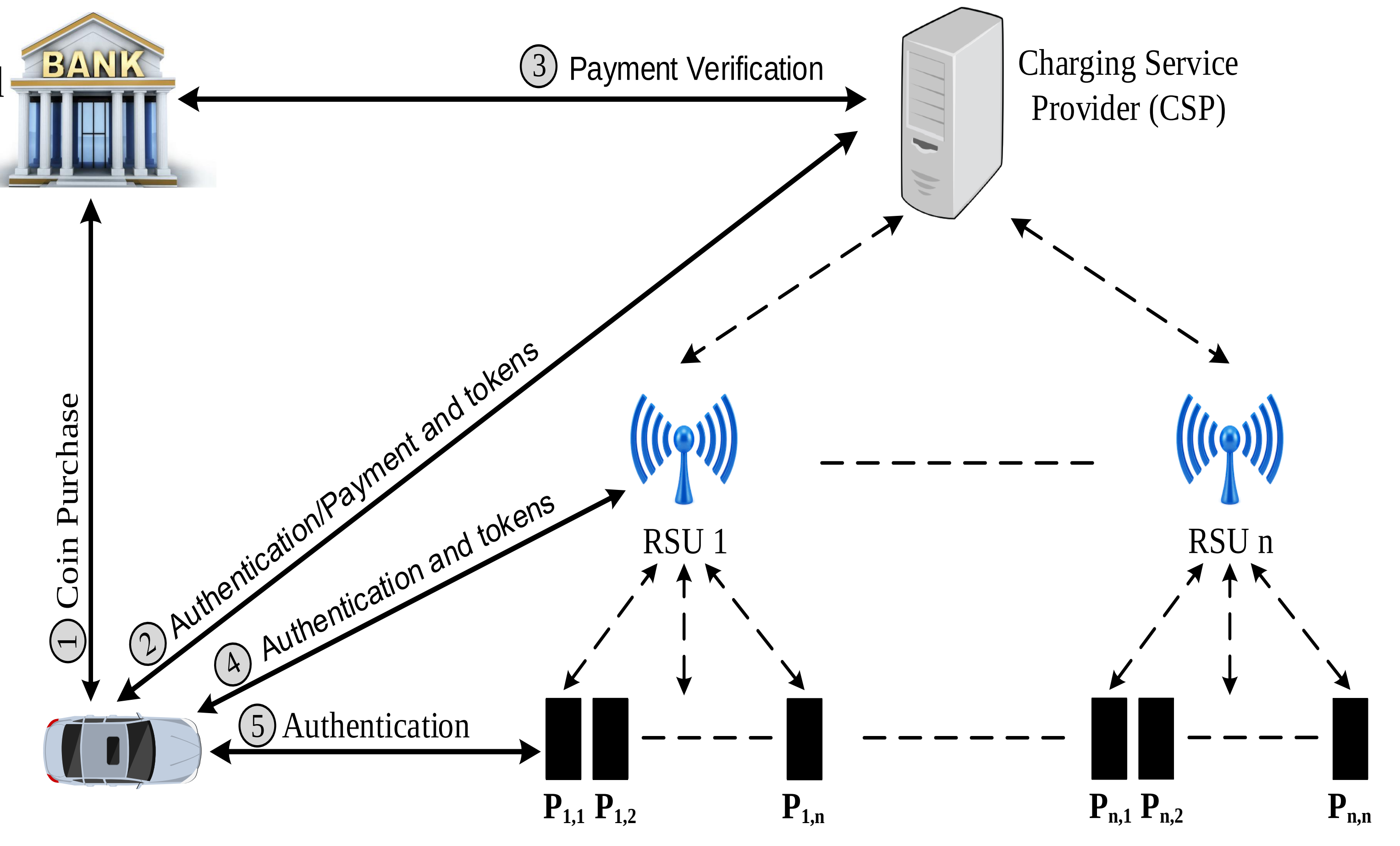

Fig 1: Network Model

5. PROPOSED SCHEME

- As illustrated in Fig. 1, the first phase in our scheme is purchasing anonymous coins shown in Fig.2 from the bank.
- When an EV needs to charge, it sends a coin to the CSP (Fig.3). The CSP needs to contact the bank to ensure that the coin has not been used before. The bank cannot link the coin to the EV that bought because of blind signature [2].
- Then, the CSP sends two secret tokens (one from Fig.4 and one from Fig.5) to enable the EV to compute shared secret keys with the RSUs as shown in Fig.6. Each RSU needs to store only one column from each matrix.
- Using these keys, the EV authenticates itself to each RSU to obtain a secret token to compute shared keys with the pads controlled by that RSU.
- The keys obtained from a RSU will be used to authenticate EV at pads under that RSU.

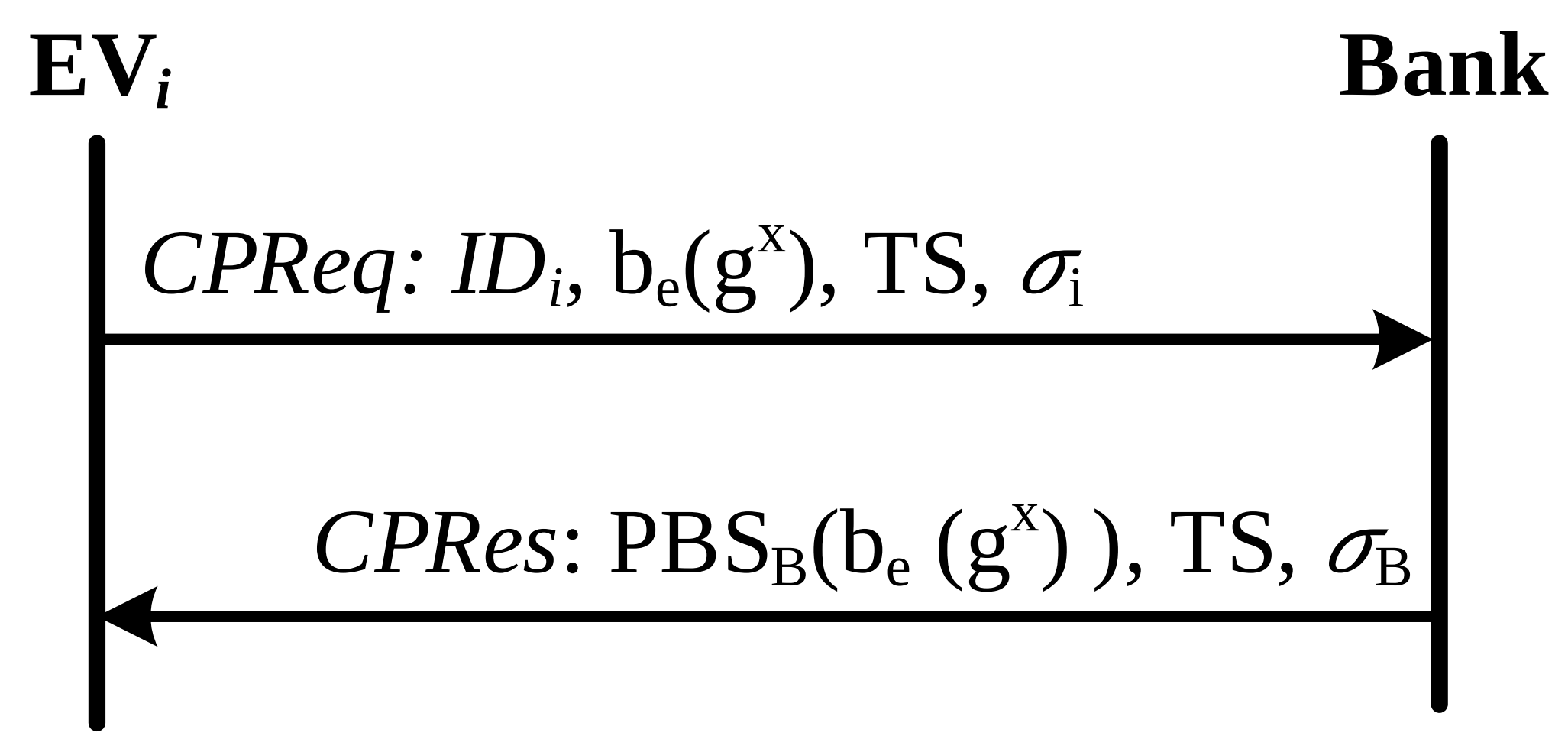
EV_i
Bank
$CPReq$: ID_i, $b_e(g^x)$, TS, σ_i
$CPRes$: $PBS_B(b_e(g^x))$, TS, σ_B

Fig 2: Purchasing Coins

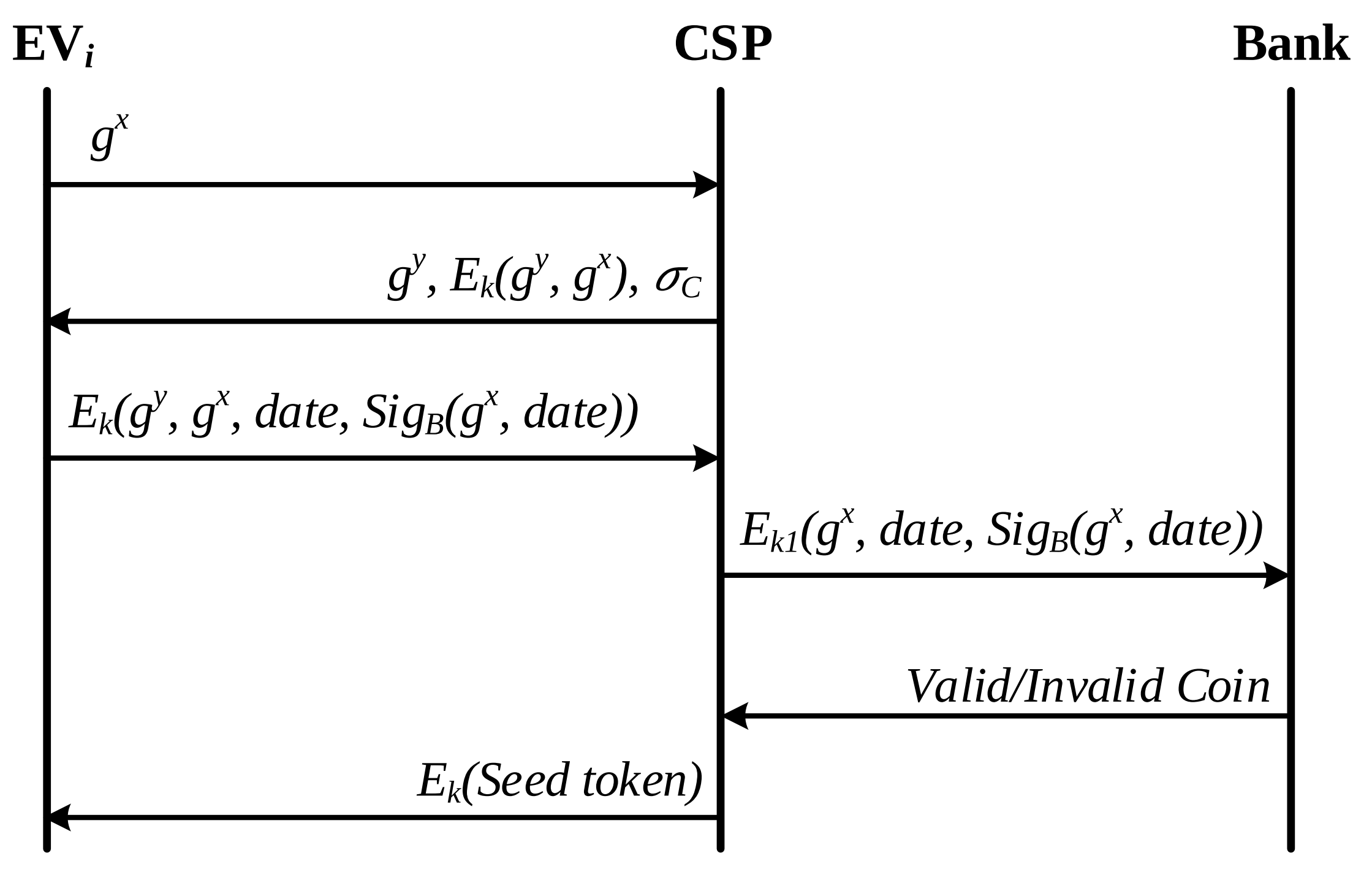
EV_i
CSP
Bank
g^x
g^y, $E_k(g^y, g^x)$, σ_C
$E_k(g^y, g^x, date, Sig_B(g^x, date))$
$E_{kI}(g^x, date, Sig_B(g^x, date))$
Valid/Invalid Coin
E_k(Seed token)

Fig 3: Authentication at Charging Station

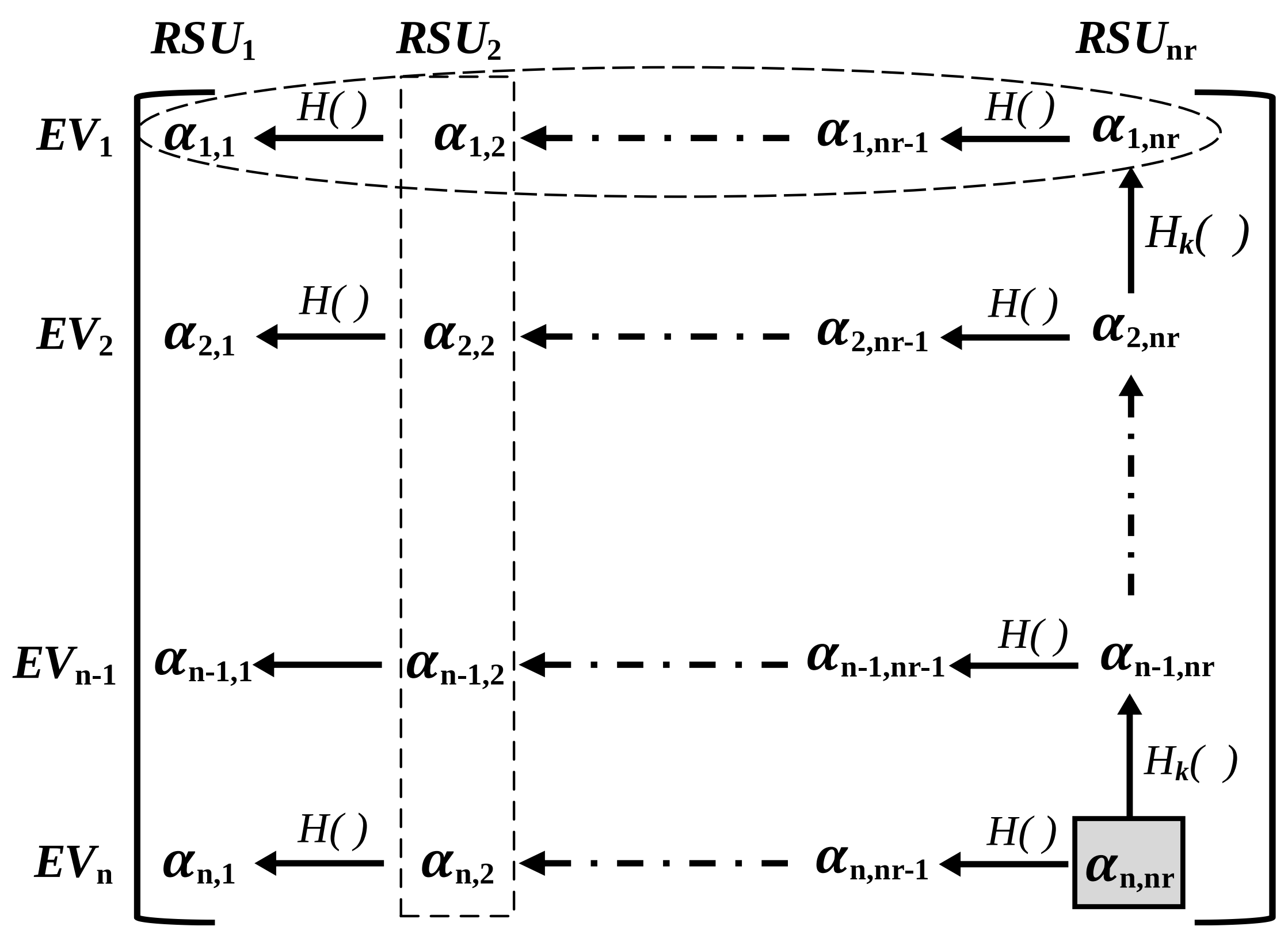
RSU_1
RSU_2
RSU_{nr}
EV_1
EV_2
EV_{n-1}
EV_n
$\alpha_{1,1}$ $\alpha_{1,2}$ $\alpha_{1,nr-1}$ $\alpha_{1,nr}$
$\alpha_{2,1}$ $\alpha_{2,2}$ $\alpha_{2,nr-1}$ $\alpha_{2,nr}$
$\alpha_{n-1,1}$ $\alpha_{n-1,2}$ $\alpha_{n-1,nr-1}$ $\alpha_{n-1,nr}$
$\alpha_{n,1}$ $\alpha_{n,2}$ $\alpha_{n,nr-1}$ $\alpha_{n,nr}$
H( )
H_k( )

Fig 4: Creating Token Matrix-1 b/w CS and RSU

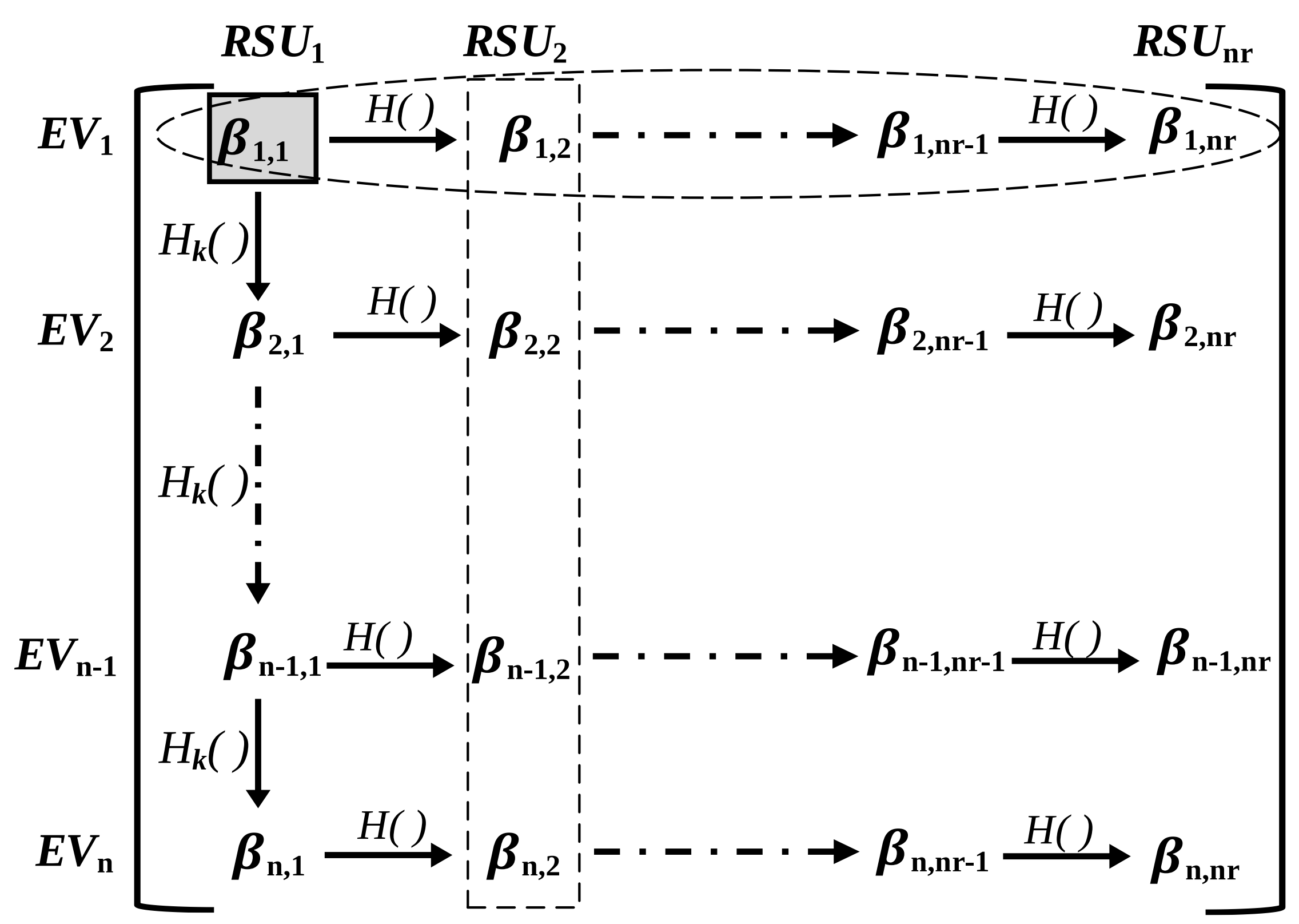
RSU_1
RSU_2
RSU_{nr}
EV_1
EV_2
EV_{n-1}
EV_n
$\beta_{1,1}$ $\beta_{1,2}$ $\beta_{1,nr-1}$ $\beta_{1,nr}$
$\beta_{2,1}$ $\beta_{2,2}$ $\beta_{2,nr-1}$ $\beta_{2,nr}$
$\beta_{n-1,1}$ $\beta_{n-1,2}$ $\beta_{n-1,nr-1}$ $\beta_{n-1,nr}$
$\beta_{n,1}$ $\beta_{n,2}$ $\beta_{n,nr-1}$ $\beta_{n,nr}$
H( )
H_k( )

Fig 5: Creating Token Matrix-2 b/w CS and RSU

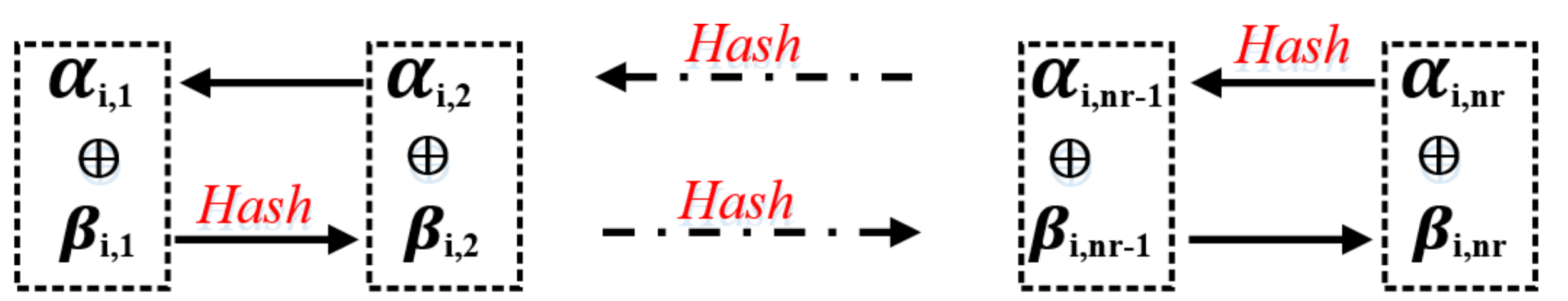
$\alpha_{i,1} \oplus \beta_{i,1}$
$\alpha_{i,2} \oplus \beta_{i,2}$
$\alpha_{i,nr-1} \oplus \beta_{i,nr-1}$
$\alpha_{i,nr} \oplus \beta_{i,nr}$
Hash

Fig 6: Computing Shared keys with RSU by EV_i

- An EV can compute the shared keys with the RSUs by hashing the two tokens given by CS and then XORing corresponding two elements, as illustrated in Fig. 6.
- Our scheme can be used to limit the number of RSUs' pads an EV can charge from by limiting the number of keys the EV can calculate, as illustrated in Fig. 7.

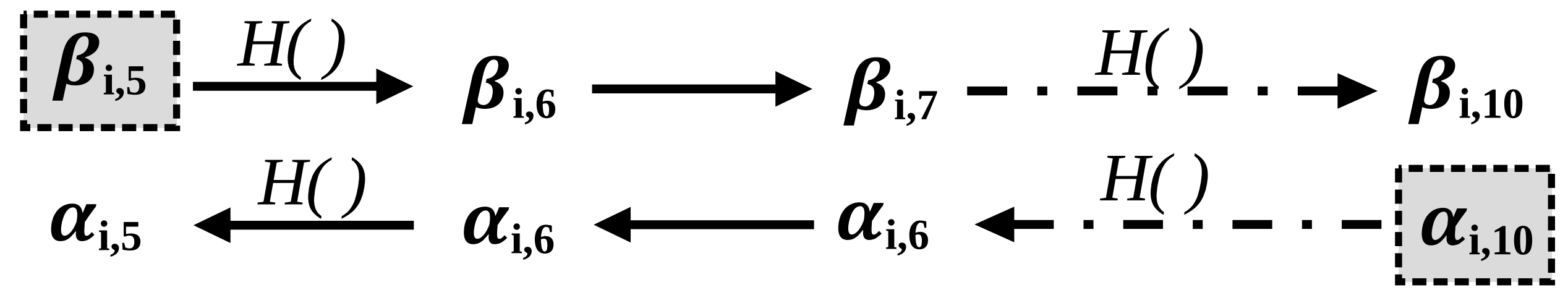
$\beta_{i,5}$ $\beta_{i,6}$ $\beta_{i,7}$ $\beta_{i,10}$
$\alpha_{i,5}$ $\alpha_{i,6}$ $\alpha_{i,6}$ $\alpha_{i,10}$
H( )

Fig 7: Charging flexibility according to Payment

- We use the same technique that is used between RSUs and CSP to enable the RSUs to share keys with the pads under their control, but by computing only one matrix by using $\gamma_{n,np}$ as seed token.

6. RESULTS

- We use two metrics, computation and communication overhead, to evaluate the performance of our scheme.
- In order to evaluate the computation overhead, we used Crypto++ 5.6.2 library [3] to measure the computation time of the cryptographic operations used in our scheme.

Entities	*Storage Overhead*	*Computation Overhead*
E.V	**($n_r \times 20$) + ($n_p \times 20$) bytes**	**0.167 μsec + 0.125 μsec**
Charging Pads	**n × 20 bytes**	**(n -1) × (n_p -1) × 0.0418μsec + 0.0418 μsec**
RSU	**n × 20 bytes**	**2 × (n -1) × (n_r -1) × 0.0418μsec + 0.23 μsec + 0.0418 μsec**
CSP	**2 × n × 20 bytes**	**2 × (n -1) × (n_r -1) × 0.0418μsec + 0.23 μsec**

7. CONCLUSION AND FUTURE WORK

The proposed scheme can secure the payment while offering full anonymity to EV drivers. We have also proposed an efficient technique to compute and share a large number of secret keys and our measurements proved it. Our scheme is scalable.

In this scheme we have treated all the EVs similarly. In future, we want to give priority levels to the EVs depending upon the attributes of each EV such as a police vehicle, ambulance or a government vehicle should get high priority than the normal EVs.

REFERENCES:

1. J. M. Miller, P. Jones, J.-M. Li, and O. C. Onar, "ORNL experience and challenges facing dynamic wireless power charging of EVs," IEEE circuits and systems magazine, vol. 15, no. 2, pp. 40–53, 2015.
2. T. Okamoto, "Efficient blind and partially blind signatures without random oracles," in Theory of Cryptography Conference. Springer, 2006, pp. 80–99.
3. Crypto++ Library 5.6.5, "Available online: https://www.cryptopp.com/."
4. H. Li, G. D´an, and K. Nahrstedt, "Portunes: Privacy-preserving fast authentication for dynamic electric vehicle charging," Proc. of IEEE International Conference on Smart Grid Communications (SmartGridComm), Venice, Italy, 3-6 Nov. 2014.

Acknowledgements : I would like to acknowledge the support of Electrical and Computer Engineering department, CESR and my advisor to do this research.