# On the Validity of Spoofing Attack Against Safe is the New Smart

Boyapally Harishma†, Urbi Chatterjee‡and Debdeep Mukhopadhyay§

## 1 Abstract

Recently, a light-weight authenticated key-exchange (AKE) scheme has been proposed. The scheme provides mutual authentication. It is asymmetric in nature by delegating complex cryptographic operations to resource-equipped servers, and carefully managing the workload on resource-constrained Smart meter nodes by using Physically Unclonable Functions. The prototype Smart meter built using commercial-off-the-shelf products is enabled with a low-cost countermeasure against load-modification attacks, which goes side-by-side with the proposed protocol. An attack against this AKE scheme has been recently proposed claiming that the server can be breached to mount spoofing attacks. It relies on the assumption that the result of an attack against authenticated key-exchange protocol is determined before the attacker learns the session key. In this short paper, we discuss the attack's validity and describe the misinterpretation of the AKE protocol's security definition.

## 2 PUF-based Authenticated Key-Exchange

Smart meters perform the useful task of 1) communicating real-time electricity price from the grid operator to the consumer, 2) reporting the consumer's day/hour ahead demand to the grid operator. One of the biggest security challenges in the Smart grid is to protect these embedded devices from security breaches that could lead to disastrous consequences. Therefore, researchers are building various authentication and key management schemes with varying security properties and resource-requirements. Several state-of-the-art PUF-based protocols targeting heterogeneous multi-party applications such as smart cards, RFID tags, and wireless sensor networks are present in the literature with more focus on the construction of a new PUF design rather than the security of the protocol.

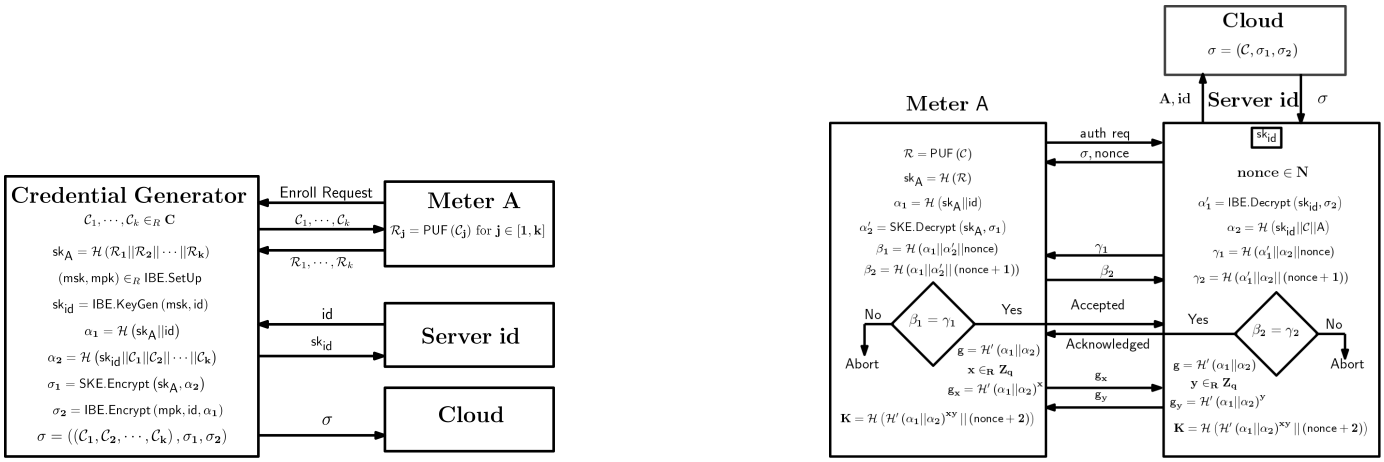
The proposed forward-secure AKE scheme is described in Fig. 1. It addresses majority of the issues in the existing literature in the context of PUF-enabled IoT devices. In particular, all PUF-enabled Smart meters in our protocol do not require any secure on-chip storage. All computations at these Smart meter nodes are run-time, resource-thrifty, and low-latency by design. It is a mutual authentication scheme, without the requirement of secure storage on the server to save the associated data related to the Smart meter for authentication. A significant part of the storage requirement is offloaded securely to a public repository (such as a cloud), in the form of associated data. The associated data is protected via cost-efficient cryptographic techniques that do not demand large challenge-response spaces for the PUF instances. The security of this protocol is formally proved using well-established cryptographic assumptions. The AKE protocol satisfies the following requirements:

- *Known Session Keys.* It must retain session key secrecy even against an adversary that may have gained some past session keys.
- *Forward Secrecy.* If secret credentials (long-term secrets) of one or more entities are compromised, the secrecy of previous session keys should not be affected.
- *Key-Compromise Impersonation.* Suppose an adversary gains access to the credentials of a given party. While this loss allows the adversary to impersonate the compromised party to all other parties, it should not allow the adversary to impersonate other parties to the compromised party.
- *Known Ephemeral Keys.* Compromise of only ephemeral (short-term) keys during a key-exchange session should not reveal the session key.

This protocol is proven to be secure using well-established cryptographic assumptions. The protocol is said to be inseucre if any PPT adversary $\mathcal{A}$, can distinguish between a valid session key from a randomly generated string with success probability that is non-negligibly smaller or greater than $1/2$. It can do so by performing one of the following tasks:

- It can either force the establishment of a second session with the same key as the target session key and then issue a key-reveal query on that session. This is the *Key-Replication Attack*.
- It is able to directly recover sufficient information about the target session key to distinguish it from the random key. This is called a *Forging Attack*.

† harishmasko@gmail.com, ‡ urbi.ism@gmail.com, § debdeep@cse.iitkgp.ernet.in




(a) Enrollment Phase

(b) Authentication and Key Exchange Phase

Fig. 1: PUF-based Authenticated Key-Exchange Protocol as presented in [1]

In other words, an attacker is said to win against the protocol, only if it can establish a valid session key with either the meter of the server for a fresh session.

## 3 Validity of the Attack Presented in [2]

In the attack model presented in [2] the attacker impersonates as a server and does the following:

1) For a previous session with nonce $= n - 1$ and $\sigma = (C, \sigma_1, \sigma_2)$: Abort the session after the attacker receives $\beta_2 = \mathcal{H}(\alpha_1||\alpha_2'||n)$ from the Smart meter. It saves $w = \beta_2$.
2) For the current session with nonce $= n$ and $\sigma = (C, \sigma_1, \sigma_2)$: Attacker sends $\gamma_1 = w$ to the Smart meter during the authentication phase.

The Smart meter accepts $\gamma_1$ as a valid message and authenticates the attacker as a legitimate server. This attack is valid ***if and only if*** the protocol ends after the authentication step, which is untrue. The proposed scheme is an authenticated key-exchange scheme, which ends after both the parties exchange the same session key. Therefore, even if the attacker can force the Smart meter to authenticate it as a legitimate device, without the knowledge of the values $\alpha_1$ and $\alpha_2$ for the corresponding $\sigma$, the attacker cannot compute $g = \mathcal{H}'(\alpha_1||\alpha_2)$ correctly, to perform Diffie-Hellman key-exchange. The attack presented in [2] also does not break any of the four requirements of the AKE protocol to generate a valid session key.

## 4 Conclusion

In summary, the attack presented in [2] against the AKE protocol proposed in [1] is invalid. It does not disprove Theorem 4.1 presented in Sec.4.3 [1], against which the AKE protocol has been proven to be secure. There is a stark distinction between the goals of an authentication protocol and an authenticated key-exchange (AKE) protocol. Therefore, we hope future papers that target on attacking existing authentication protocols, key-exchange protocols, AKE protocols or any other protocols comprehensively understand the threat model, design goals and the security definition against which the protocol is proven to be secure.

## References

[1] H. Boyapally, P. Mathew, S. Patranabis, U. Chatterjee, U. Agarwal, M. Maheshwari, S. Dey, and D. Mukhopadhyay. Safe is the new smart: Puf-based authentication for load modification-resistant smart meters. *IEEE Transactions on Dependable and Secure Computing*, pages 1–1, 2020.
[2] K. Lounis. Security of Short-Range Wireless Technologies and an Authentication Protocol for IoT. Master's thesis, Queen's University,Kingston, Ontario, Canada, Canada, 2021.