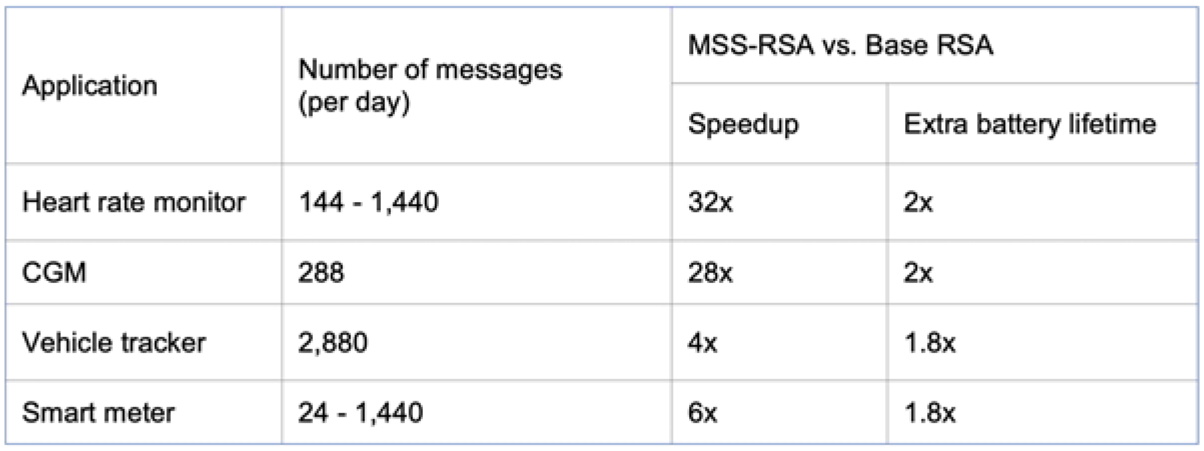
Lightweight Network Authentication For Resource Constrained Devices

Tech ID: 33233 / UC Case 2021-824-0

CONTACT

Venkata S. Krishnamurty
venkata.krishnamurty@ucr.edu
tel: .

BRIEF DESCRIPTION



Application	Number of messages (per day)	MSS-RSA vs. Base RSA	
		Speedup	Extra battery lifetime
Heart rate monitor	144 - 1,440	32x	2x
CGM	288	28x	2x
Vehicle tracker	2,880	4x	1.8x
Smart meter	24 - 1,440	6x	1.8x

Efficiency gains for a few sample applications; CGM = Continuous Glucose Monitor; MSS = Mergeable Stateful Signatures.

OTHER INFORMATION

KEYWORDS

authentication, Internet of things, network security, one time password, IoT, OTP, cyber-physical security

CATEGORIZED AS

- Security and Defense
  - Cyber security

RELATED CASES

2021-824-0

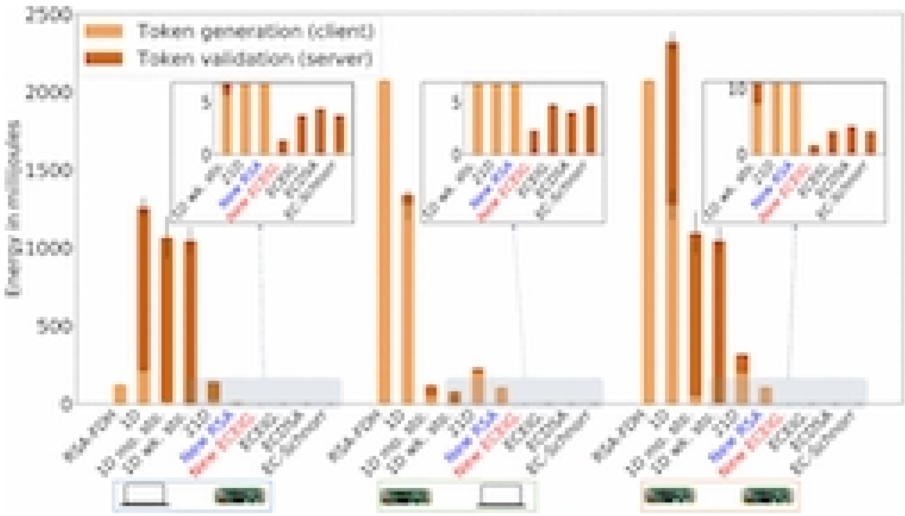
FULL DESCRIPTION

Background

Authentication is a central challenge in secure protocol design for edge devices. The IoT environment often has a special system model in which IoT devices frequently communicate a small amount of authenticated data to a single server. IoT devices are often powered by batteries - so the authentication solution must not consume high energy. Symmetric key cryptography that is often used, imposes key-management issues and introduces security vulnerabilities. Authentication based on hash chains has a lifespan and requires expensive computation.

Technology

Research team at UCR led by Prof. Nael Abu-Ghazaleh have designed a novel signature/authentication scheme called Mergeable Stateful Signatures (MSS) that provides an authentication protocol with low overhead. The team has derived MSS instantiations for two cryptographic families, assuming the hardness of RSA and decisional Diffie-Hellman (DDH) respectively, thereby demonstrating the generality of the design. They have also implemented two time-based one-time password (TOTP) authentication systems from the RSA and DDH instantiations.



Comparison of authentication energy consumption of TOTP systems.

ADVANTAGES

- The implementation of RSA-TOTP system reduces authentication latency by 6X and energy consumption by 10X.
- The implementation of ECElGamal-TOTP system reduces authentication latency by 82X and energy consumption by 792X compared to hash chain based TOTP system.
- MSS is versatile - it reduces the signature verification cost when client-server roles are switched and the IoT device becomes the server/verifier.

SUGGESTED USES

Resource constrained edge devices such as:

- Medical devices such as heart rate monitor, continuous glucose monitor, etc.
- Drone command and control.
- Sensors.
- Infrastructure related devices such as smart meters, etc.

RELATED MATERIALS

- MSS: Lightweight network authentication for resource constrained devices via Mergeable Stateful Signatures

INVENTOR INFORMATION

- Please read recent news coverage of Prof. Nael Abu-Ghazaleh
- Please visit Prof. Abu-Ghazaleh's profile page to learn more about his research.
- Please review all inventions by Prof. Abu-Ghazaleh and his team at UCR.

PATENT STATUS

Country	Type	Number	Dated	Case
United States Of America	Published Application	20230034512	02/02/2023	2021-824

University of California, Riverside
Office of Technology Commercialization
200 University Office Building,
Riverside,CA 92521
otc@ucr.edu
research.ucr.edu/