Whitenoise can be deployed in hardware contexts where RSA cannot go

As with all technologies, the eventual competitive battles devolve to price wars. Unfortunately when security is part of what should be delivered along with performance, the biggest corporations and institutions in the world often trade or sacrifice security for speed and other more marketable metrics.

This trade off is not necessary with Whitenoise technologies. You can have both.

This paper examines the cost comparison (as well as the technological capability) of Whitenoise security deployed from low cost processing components like PICs, registers, counters, circular shift registers and line feed shift registers and the impossibility, scientifically, of deploying RSA-style asymmetric, public key cryptosystems in those low power, low computational, low overhead components.

Intel has adopted AES NI (new instructions) because they needed more speed and the new instructions offloads some of the more complex arithmetic calculations of public key technologies to the chip. In this paper http://www.wnlabs.com/downloads/Comparison_of_handshakes.pdf we can see the challenge that exists.

Whitenoise is orders of magnitude faster and stronger than the best encryption algorithm that RSA has to offer: http://www.wnlabs.com/pdf/Internet_of_Things_and_Whitenoise_Technologies.pdf

Whitenoise can easily be deployed in more places:
http://www.wnlabs.com/downloads/Whitenoise_Usage_scenarios.pdf

The biggest growing threat to our security is the exploding points of egress vulnerability of low-cost communicating endpoints on our networks. NO MANUFACTURER can pay > $10 per chip for a smart component whose retail cost is targeted from a couple of dollars (i.e. a thermostat) to < $30. It would be suicide. The Internet of Everything will be characterized by products whose retail cost is between $2 and $30.

Let's look at the current market and cost of chips for mobile devices.

The cost of the chip and modem for an Apple iPhone is estimated at $59.50 and the processor is estimated to cost $37. And its security has been regularly questioned.
http://www.techinsights.com/teardown.com/apple-iphone-6

Cost comparison between typical chipsets and peripheral interface controllers

Preliminary analysis of the iPhone 6 Plus estimates it costs $242.50 USD to build - an increase of about 15% more than the iPhone 5S. The estimated combined cost of Apple's new A8 processor and Qualcomm's MDM9625M modem account for $59.50 of the preliminary CoG, while the 5.5" display / touchscreen assembly costs another estimated $51.00. For the iPhone 6 the preliminary display / touchscreen cost about $41.50 with the iPhone 6 total CoG to be approximately $227.00.

Intel processors are expensive and have made their own possible tradeoffs by implementing AES NI. The focus is speed while doing little to improve or address security flaws in the underlying framework.

The [Intel price list](#) shows their cheapest chipset to be in the range of $40. This cost alone surpasses the overall targeted costs of competitive IoT components.

Intel® Celeron® processor Desktop (LGA1150/LGA1155)	June'15 (06/07) Price	Aug'15 (08/05) Price	% Decrease
G1850 (2M cache, 2 Cores, 2 Threads, 2.90 GHz, 22nm)	$52	$52	-
G1830 (2M cache, 2 Cores, 2 Threads, 2.80 GHz, 22nm)	$52	$52	-
G1840 (2M cache, 2 Cores, 2 Threads, 2.80 GHz, 22nm)	$42	$42	-
G1820 (2M cache, 2 Cores, 2 Threads, 2.70 GHz, 22nm)	$42	$42	-

Intel® Core™ i7 processor Mobile (FCPGA10/Socket G2, FCBGA10)	June'15 (06/07) Price	Aug'15 (08/05) Price	% Decrease
i7-4910MQ (8M cache, 4 Cores, 8 Threads, 2.90 GHz, 22nm)	$568	$568	-
i7-4900MQ (8M cache, 4 Cores, 8 Threads, 2.80 GHz, 22nm)	$568	$568	-
i7-4810MQ (6M cache, 4 Cores, 8 Threads, 2.80 GHz, 22nm)	$378	$378	-
i7-4800MQ (6M cache, 4 Cores, 8 Threads, 2.70 GHz, 22nm)	$378	$378	-
i7-4712MQ (6M cache, 4 Cores, 8 Threads, 2.30 GHz, 22nm)	$378	$378	-
i7-4710MQ (6M cache, 4 Cores, 8 Threads, 2.50 GHz, 22nm)	$378	$378	-
i7-4610M (4M cache, 2 Cores, 4 Threads, 3.00 GHz, 22nm)	$346	$346	-
i7-4600M (4M cache, 2 Cores, 4 Threads, 2.90 GHz, 22nm)	$346	$346	-
i7-5950HQ 6M cache, 4 Cores, 8 Threads, 2.90 GHz, 14nm)	$623	$623	-
i7-4980HQ (6M cache, 4 Cores, 8 Threads, 2.80 GHz, 22nm)	$623	$623	-
i7-4960HQ (6M cache, 4 Cores, 8 Threads, 2.60 GHz, 22nm)	$623	$623	-
i7-4950HQ (6M cache, 4 Cores, 8 Threads, 2.40 GHz, 22nm)	$623	$623	-
i7-5850HQ (6M cache, 4 Cores, 8 Threads, 2.70 GHz, 14nm)	$434	$434	-
i7-4870HQ (6M cache, 4 Cores, 8 Threads, 2.50 GHz, 22nm)	$434	$434	-
i7-4860HQ (6M cache, 4 Cores, 8 Threads, 2.40 GHz, 22nm)	$434	$434	-
i7-4850HQ (6M cache, 4 Cores, 8 Threads, 2.10 GHz, 22nm)	$434	$434	-
i7-5750HQ (6M cache, 4 Cores, 8 Threads, 2.50 GHz, 14nm)	$434	$434	-
i7-5700HQ (6M cache, 4 Cores, 8 Threads, 2.70 GHz, 14nm)	$378	$378	-
i7-4770HQ (6M cache, 4 Cores, 8 Threads, 2.20 GHz, 22nm)	$434	$434	-
i7-4760HQ (6M cache, 4 Cores, 8 Threads, 2.10 GHz, 22nm)	$434	$434	-
i7-4712HQ (6M cache, 4 Cores, 8 Threads, 2.30 GHz, 22nm)	$378	$378	-
i7-4710HQ (6M cache, 4 Cores, 8 Threads, 2.50 GHz, 22nm)	$378	$378	-

Cost comparison between typical chipsets and peripheral interface controllers

Whitenoise technologies, Dynamic Identity Verification and Authentication (DIVA) and Dynamic Distributed Key Infrastructure virtual frameworks is **the ONLY national security level cryptosystem that can be deployed in low cost microprocessing environments** like Peripheral Interface Controllers (PICs).

Z80A-PIO: Parallel I/O Interface Controller 4MHZ DIP-40 (Zilog Series)

Parallel I/O Interface Controller 4MHz Dip-40

Part no. 35641	
Product Category	Microprocessors
Product Type	Zilog Series
Manufacturer	Major Brands
Manufacturer no.	Z80A-PIO
Overview	IC, Z80A-PIO(MK3881N-4)

Availability: Ship today

From **$2.25** each

1+ $2.25
10+ $1.95
100+ $1.75

QTY 1

ADD TO CART

The above cost is a retail cost. PICs and things like RFID tags can be manufactured at approximately $ .20 - $ .40 a unit while offering the highest level of security available.

--

There are two ways to look at this cost disparity.

1. There are entire IoT and smart markets where RSA and asymmetric technologies just can't be deployed because of scientific and cost realities.

2. Companies like Intel have likely invested billions of dollars into their AES NI efforts. Adding Whitenoise to their AES NI chipsets would improve their security by orders of magnitude while only adding less than a dollar to their manufacturing cost.