PAEQ v1:
Clarification on recommended parameter sets

Designers: Alex Biryukov and Dmitry Khovratovich
University of Luxembourg, Luxembourg

Submitters: Alex Biryukov and Dmitry Khovratovich
alex.biryukov@uni.lu, dmitry.khovratovich@uni.lu, khovratovich@gmail.com

https://www.cryptolux.org/index.php/PAEQ

19th March, 2014

This documents explicitly orders the recommended parameter sets by priority and provides the security goals for them.

Recommended parameter sets

We recommend the following parameter sets (in bits) depending on the user's requirements to the overall security level and the need of extra features of nonce-misuse resistance and quick tag update.

Priority	Name	Key length	Nonce length	Tag length	Comment
1	`paeq128`	128	96	128	128-bit security
2	`paeq64`	64	64	64	64-bit security
3	`paeq80`	80	80	80	80-bit security
4	`paeq128-t`	128	128	512	128-bit security with quick tag update
5	`paeq128-tnm`	128	256	512	128-bit security with nonce-misuse and tag update options
6	`paeq160`	160	128	160	160-bit security

The reference implementation can be easily tuned to support other parameter sets, e.g. (256,128,128) for 128-bit security with 256-bit keys.

Security goals

Here we formulate the security goals for our recommended parameter sets.

	Cipher					
	`paeq64`	`paeq80`	`paeq128`	`paeq128-t`	`paeq128-tnm`	`paeq160`
Confidentiality for the plaintext	64	80	128	128	128	160
Integrity for the plaintext	64	80	128	128	128	160
Integrity for the associated data	64	80	128	128	128	160
Integrity for the public message number	64	80	128	128	128	160