From:	渡邊榮治(Eiji Watanabe)(メテオーラシステム)
To:	pqc-comments
Cc:	pqc-forum@list.nist.gov
Subject:	OFFICIAL COMMENT: Post-quantum RSA-Encryption
Date:	Monday, January 28, 2019 7:59:22 AM
Attachments:	Table.pdf Dear submitters of Post.pdf

Dear Post-quantum RSA team and Dear all
Hello, I am very happy to have the opportunity to express my opinion about your drastic posting.

I like RSA team postings very much. Of course there are reasons: Let's assume that there is mathematics called the ideal Post-Quantum Crypto(PQC). The ideal PQC here is defined as a triple thrust that convenience is good, reliability is good and implementation is easy. Sooner or later, we will begin looking for mathematics with that triple. In the meantime, there is a possibility of encountering *credit crunch* from the Internet. This is because we cannot argue against those who dispute the verification ability of the log. So, we must ask a person with a foresight, now: Do you take more convenience than *reliability*? Do you take easier to implement than *reliability*? Or are you looking for optimum values of the triple thrust rather than *reliability*?

I will choose the reliability of the public key more than anything. Even if the convenience is bad, if reliability is guaranteed, the world economy will rebound from *the credit crunch* like overcoming the Reaman shock. Conversely, the background of *credit concern* is not a matter of convenience, it is not a matter of gap between optimal values, it is not a problem of ease of implementation, but it is *just a lack of reliability!* In that sense I like pqRSA.

There is another reason: There is no one who doubts the reliability of RSA and pqRSA. This is the most important issue in avoiding *credit crunch*. Instead, convenience is sacrificed. For example, click & response becomes heavy. There is salvation: When deploying pqRSA to the application, let's implement a hybrid of my invention and pqRSA. This will make click & response the same speed as the current browser. The security provided here is *Forward secrecy* for encryption keys: when integrating the cipher text on the communication line, You will see that the algorithm for erasing the cryptographic key [Zn] works with the encryption key [Zn] itself and so mathematics and Intel's RDRAND guarantee the existence of that algorithm. What I have described here is related to the first step to avoid *credit crunch*.

Finally there is a third reason: Last year, I went back to the 1970s and mapped the key delivery scenario to a random variable expression. What came out was *a formula proving the origin of the public key*. In addition to this formula there is no mathematics to support quantum resistant public key: quantum resistant public key is a hypothesis. Disclose this formula in one sheet ☛ Attached PDF. This table suggests that pqRSA may survive.

Best regards
Eiji Watanabe

Operation $p - q = 0$ does not guarantee quantum resistance

Key delivery scenario	Operation which double key multiplication	
	$p - q \neq 0$	$p - q = 0$
Symmetric system	DES AES	XOR operation D-H protocol
Asymmetric system	A pre-image x1 to n codes	RSA public key Quantum-resistant public key
One-way stronghold	Collision difficulty	Difficulty in prime factorization
Survive in the era of quantum computers	○	✕ : compared to ○ excluding pqRSA

It is a table that I analyzed key delivery scenario back in the 1970's.