**Nigel Smart, Professor of Cryptology,**
**Dept. of Computer Science,**
Merchant Venturers Building
Woodland Road
BRISTOL
BS8 1UB
T +44 117 954 5163
F +44 117 954 5208
nigel@cs.bris.ac.uk

Rene Peralta and John Kelsey,
National Institute of Standards and Technology,
Computer Security Division.

June 13, 2016

Dear Rene and John,

This note follows on to our earlier discussion and your related request for input from other organizations who would welcome NIST development of new cryptographic standards. As an interested group of experts in cryptography, we advocate establishing standards of higher level cryptographic elements than the block cipher and other primitives that NIST has traditionally standardized. Below, we identify and prioritize what we feel are the salient higher-level elements to consider for new standards..

**Secret sharing** refers to the distributed storage and computation on data by representing that data as a collection of cryptographic shares, such that individual shares reveal nothing about the original data, but recombination of a certain number of those shares can be used to re-create the original data. The basic concept of secret sharing was developed by Shamir in 1979. Since then, a wide variety of schemes have been published, leaving a technology landscape full of incompatible constructions that offer varying performance and security guarantees. Recently, secret sharing has been commercialized for use in protecting cryptographic keys at rest, performing tax fraud analysis on untrusted servers while protecting the data in use, and providing verification of web service message authentication codes for data in transit. ISO is currently aiming to standardize some aspects of secret sharing in SC27 to form ISO19592-2. The draft ISO standard includes a number of schemes primarily in the areas of thresholds for recovering data from shares and replication schemes.

However, certain capabilities seem to be excluded from the draft standard that we feel will be important for successful broad commercialization of secret sharing technology. For example, although traditional Shamir sharing has an efficient, concise representation, distributing shares among shareholders is expensive because of the need for secure channels between all players. A different sharing approach, pseudo-random secret sharing (PRSS) allows share distribution using a single broadcast, thus reducing communication cost and latency and improving performance. PRSS achieves this advantage by use of previously distributed and re-usable pseudo-random functions, or seed values for such functions. The ISO draft standard for secret sharing unfortunately does not address PRSS technologies.

Because NIST has interests in assuring security of cryptographic keys and data, standardization of secret sharing technology seems aligned with NIST goals and beneficial to commercialization of useful cryptography.

**Zero Knowledge (ZK) Proofs** are methods where one party can prove to another that an assertion is true, without conveying any secret information in support of that assertion. Zero knowledge proofs have several emerging applications. For example, user authentication using a credential such as a cryptographic key can be achieved using zero knowledge in such a way that the credential need not be disclosed by the user to the authenticator. Despite being used in a number of niche applications today (UProve, Idemix, TPMs, plus a number of closed proprietary systems) there is no standard for zero knowledge proofs. Some ISO standards touch on it, but often in a confused and haphazard manner. We believe that companies would prefer a standard to reference for such basic ZK schemes. For example simple Sigma protocols for equality and/or relationships of DLP/Pedersen commitment properties would be useful in known-order groups. In particular, it would be useful to have standard defining how to take the Sigma protocol and make it non-interactive (something engineers often get wrong).

**Oblivious Transfer (OT)** is a basic building block in some cryptographic protocols. For example, OT is a fundamental building block for secure two-party computation using garbled circuit approaches. We believe that a standard including one or two "known-good" protocols would be a useful start.

**Garbled Circuit Construction** is a key building block in many two-party secure computation protocols. Techniques here are well-known, but tend to be incompatible and thus not amenable to common programming interfaces (APIs) or software libraries. Standards in this area may be needed quite soon to assure interoperability among multi-party computation products emerging from several companies such as Cybernetica, Dyadic Security, Partisia, Sepior, and SAP.

We believe that standards for the first two of these technologies are very much needed at the moment. We believe that the latter two technologies would benefit from standardization in the not-too-distant future, to assure interoperability and composability of cryptographic elements.

Yours Sincerely,

Prof. Nigel Smart,

on behalf of,

Dave Archer, Research Lead, Galois Inc., USA,
Dan Bogdanov, R&D Team Lead, Cybernetica, Estonia,
Philip Bond, Chief Cryptographer, SETL, United Kingdom,
Joppe Bos, Cryptographer, NXP Semiconductors, Belgium,

Jan Camenisch, Principal Research Staff Member, IBM, Switzerland,
George French, VP Security Architecture and Engineering, Barclays Bank, United Kingdom,
Florian Kerschbaum, Chief Research Expert, SAP, Germany,
Kristen Lauter, Principal Researcher and Research Manager, Microsoft, USA,
Kurt Nielsen, CEO, Partisia, Denmark,
Jakob Illeborg Pagter, CTO, Sepior, Denmark,
Guy Peer, CTO, Dyadic Security, Israel,
Mike Scott, Chief Cryptographer, Miracl, United Kingdom.