Web Cryptography API vNext should add BigNum support

Brian A. LaMacchia

In March 2013 during the development of v1 of the W3C Web Cryptography API, Microsoft submitted to the Web Cryptography Working Group a proposal to add support for arbitrary-precision integers -- a.k.a. "BigNums" -- to the WebCrypto API (see [1] for the original proposal). Arbitrary-precision integers are needed for general finite-field and elliptic curve mathematical operations beyond the basic public-key encryption, decryption, signature generation and verification APIs provided in the standard. For example, BigNum support is needed in order to implement the client-side protocol of the U-Prove [2] anonymous credential technology.

Although there are clear use cases requiring low-level BigNum support, the Web Cryptography Working Group declined to include such support in v1 of the standard, instead suggesting that standardization should occur at the JavaScript language level.

Since that time, Microsoft Research has continued to work on BigNum support for JavaScript and advanced cryptographic protocols that need such support. Recently we released an open-source JavaScript Cryptography Library [3] that includes a revised implementation of the arbitrary-precision integer proposal, support for both finite-field and elliptic curve mathematical operations, and uses that functionality to implement the v1 Web Cryptography API. Building on the JavaScript Cryptography Library and its BigNum support, we have written and released a U-Prove JavaScript SDK that implements the U-Prove client-side protocol (see [4]). These two libraries demonstrate the clear value of having BigNum support included in the Web Cryptography API.

Given that the primary use of arbitrary-precision integer operations over finite fields is cryptography, it was a mistake for the Web Cryptography Working Group to not include such support in v1 of the standard and this omission should be explicitly included as in scope for any re-chartering of the Web Cryptography Working Group.

[1] http://lists.w3.org/Archives/Public/public-webcrypto/2013Mar/0029.html

[2] http://research.microsoft.com/en-us/projects/u-prove/

[3] http://research.microsoft.com/en-us/downloads/29f9385d-da4c-479a-b2ea-2a7bb335d727/default.aspx

[4] http://research.microsoft.com/en-us/downloads/1008a07e-5cc6-4a96-a6f1-4f26dadb317b/