Dear Sirs,
We are pleased to DESIGN the Digital US Dollar Project using Your Picnic for deploying Our ReEncryption Keychain instead of Blockchain.
Sincerely yours,
Makoto Saito in Japan
The U.S. patents listed as covering the MQDSS submission, US 8,522,033 and US 8,959,355, cover various categories of identification schemes and signature schemes where the public key is the result of applying “a multi-order multi-variable polynomial” to the secret key.

(US 8,522,033 contains typographical errors in which “y-f(s)=0” is written as “y=f(s)=0”; that error does not occur in US 8,959,355.)

LowMC is a multi-variable, multi-order polynomial, and all of the Picnic, Picnic2, and Picnic3 signature schemes and identification schemes appear to be covered by various claims of both patents.

Robert Ransom