Notes on Paper “Efficient Multi-party Digital Signature using Adaptive Secret
Sharing for Low-Power Devices in Wireless Networks”


For this paper, we think that one clarification is deemed necessary and one typo error in
an important equation should be corrected in the original paper although the corresponding
conference proceedings record (c.f. reference [2] of the original paper) of the same topic is
correct in this regard. We would like to make the following notes and corrections to the paper.

1. Let the number of participating signers be $t+1$, then originally, the message digest $c$
defined in Item 2) under Algorithm 10 in page 886 has an inexplicitly sign dependent on $t$; however, we believe that it is a better idea to make it explicit. Otherwise, when $t$ is an
odd number, the minus operator in Equation (6) and that in the equation under Item 4) in Algorithm 10 in Page 886 remain the same, they could be mistakenly thought to
be a plus operator when $t$ is an even number. While these two equations hold the same
as before, the message digest $c$ in Item 2) in Algorithm 10 is instead defined as follows:

$$c = (-1)^{t+1} H(m, r_x)$$  \hspace{1cm} (1)

2. One typo error (product vs sum) is introduced in the equation under Item 4) in Algo-
rithm 10 in Page 886. It should be corrected as follows:

$$\text{SIG}_i = \left\{ \text{sig}_j \left| (\text{sig}_j)^T = r_j - c \prod_{t \neq j} w_t (w_j - w_t)^{-1} y_j \right. \right\}$$ \hspace{1cm} (2)

One side comment is that this multi-party signature scheme supports any larger than $t$
number of non-disqualified players under A-ECDKG participating for a multi-party signature.
When a group of $t_p$ ($t_p > t$) MiDS signers are participating in this multi-party signature
scheme, the algorithm follows these exactly same steps (note that the message digest $c$ is
defined with $t_p$ replacing $t+1$ in Equation (1) as shown above), and the product operators in
these two aforementioned equations in Algorithm 10 will be instead multiplying $r_p - 1$ terms.
by a signer, and the final signature will be the summation of all these partial signatures in \( \text{SIG}_i \) under a successful execution of MiDS.

As this note is largely clarifying the existing scheme, it does not affect the outcome of its security nor its performance. Since MiDS follows the standalone version of Schnorr, to a large degree, MiDS inherits the same type of vulnerability.