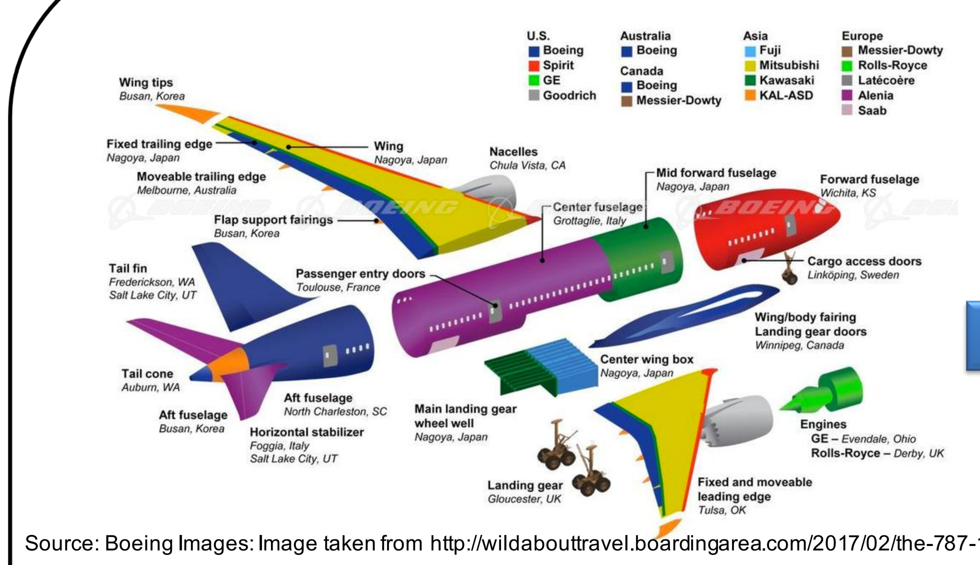
CERIAS

The Center for Education and Research in Information Assurance and Security

Lightweight, Scalable and Secure Computations for Engineering Design

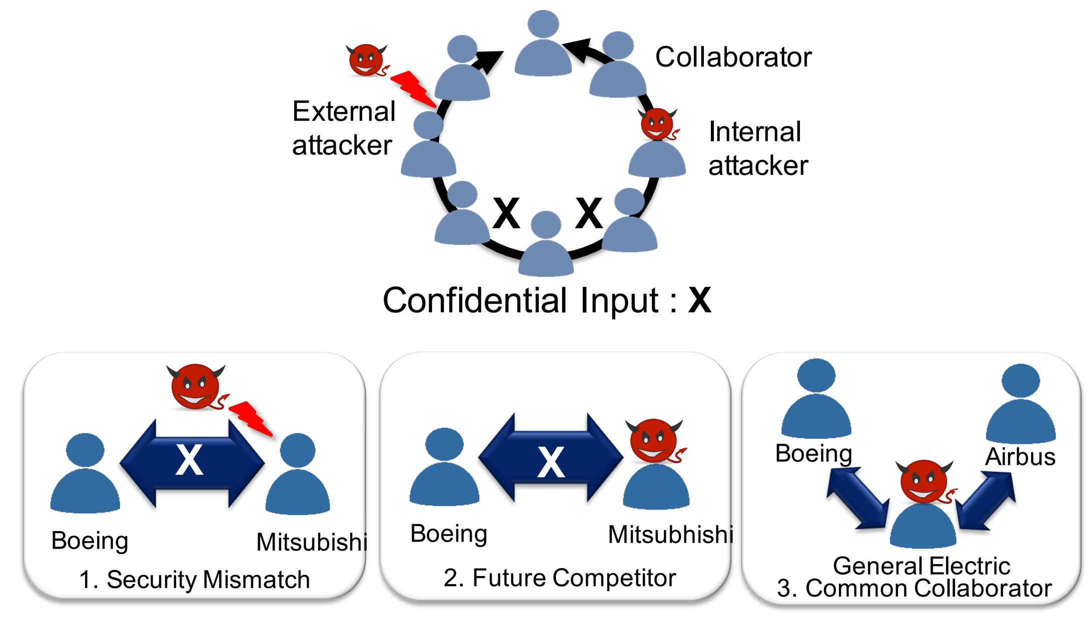
Siva C. Chaduvula, Mikhail J. Atallah, Jitesh H. Panchal
Purdue University

Motivation



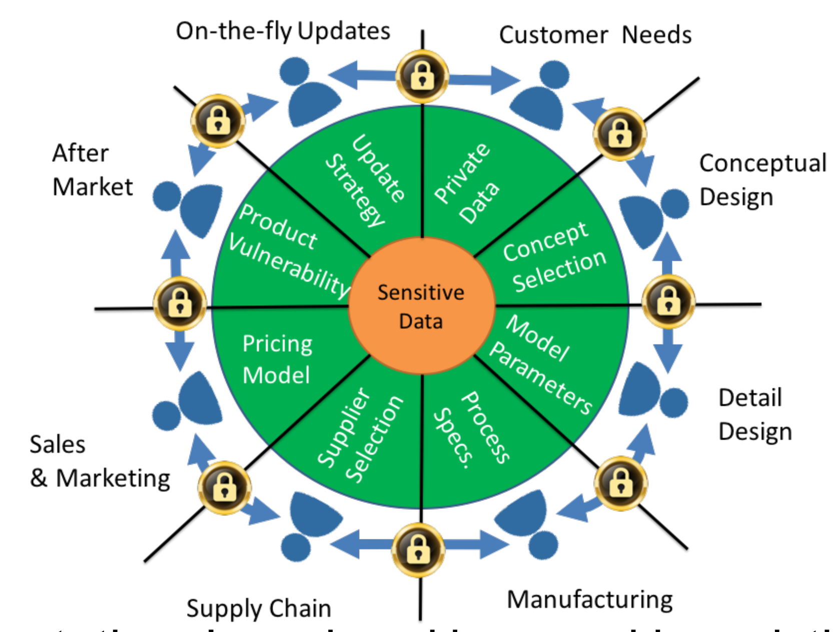
Source: Boeing Images: Image taken from http://wildabouttravel.boardingarea.com/2017/02/the-787-10/

Engineering collaborations involve sensitive information flow among designers from different enterprises from multiple countries



Note: Enterprises mentioned in this slide are purely for illustrative purposes

Information shared is prone to leakage and misuse through collaborators



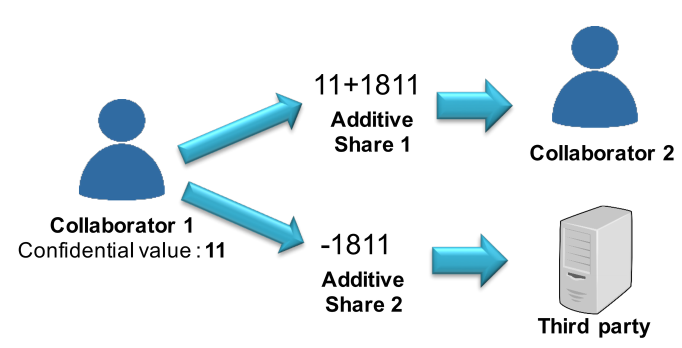
Computational overhead imposed by existing cryptographic approaches make them unsuitable for intensive and iterative engineering computations

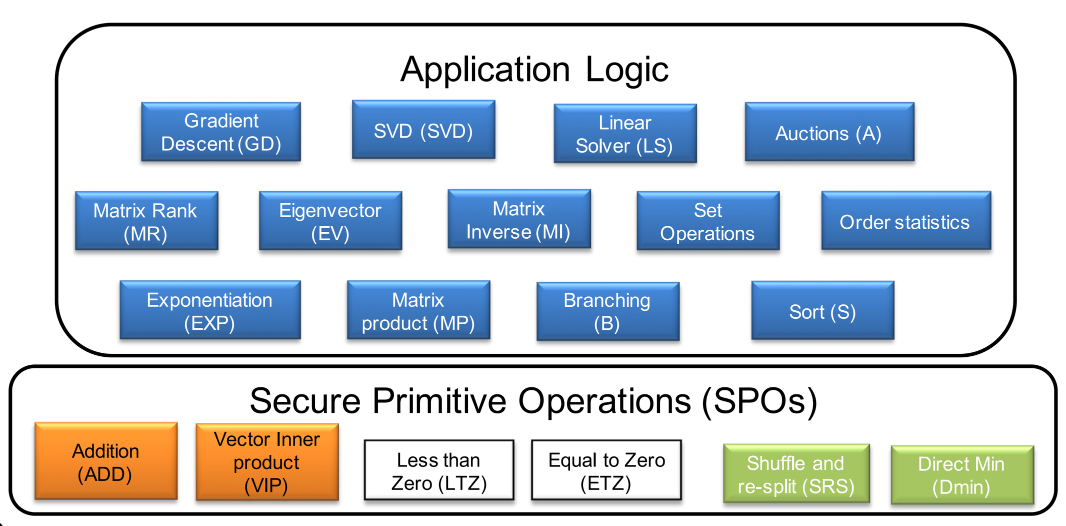
RQ: How can designers execute their computations securely and efficiently in a co-design setting?

Approach & Results

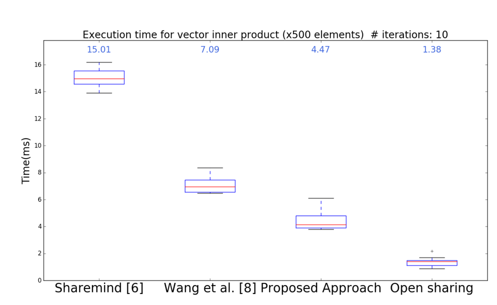
Fast Lightweight And Secure Computations (FLASC)

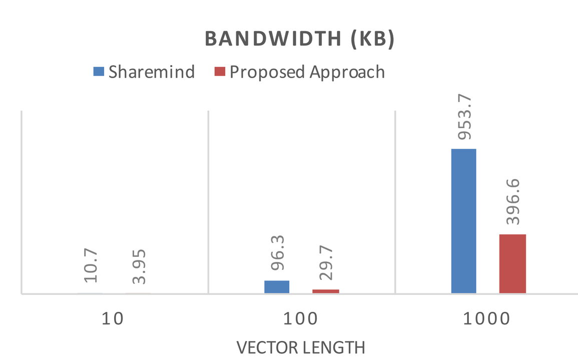
- Adding/multiplying a parameter with a large random number hides the parameter
- Adding or multiplying a large number is orders of magnitude faster than existing cryptographic primitives that rely on modular exponentiation





SPOs Performance

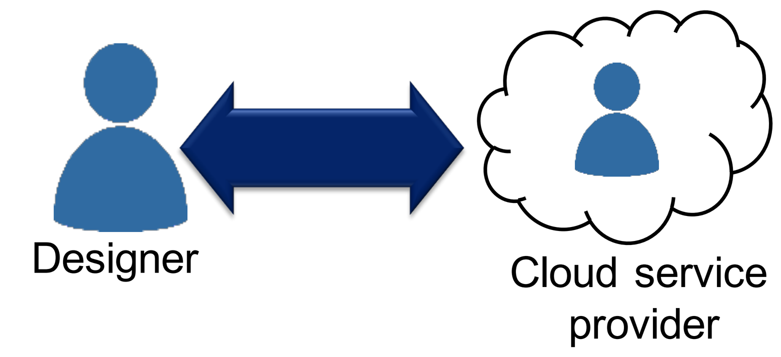




Scalability (VIP)

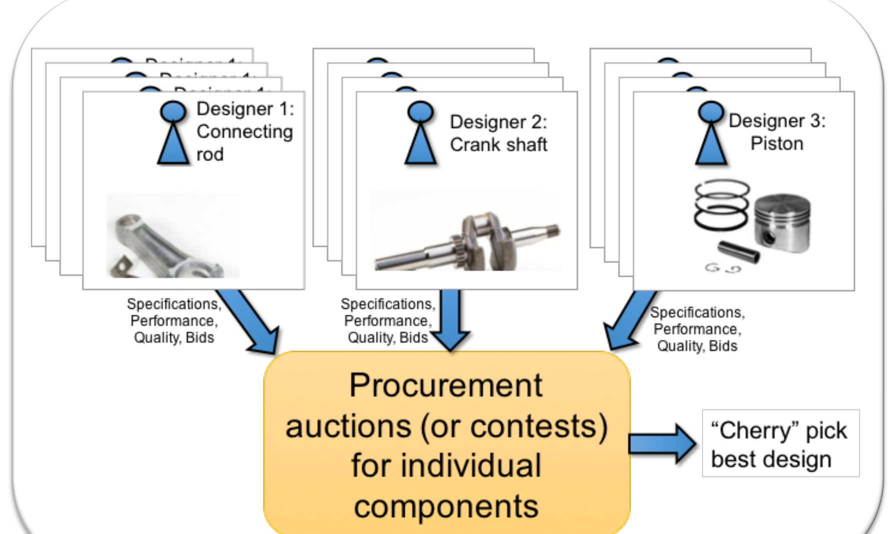
Broader Impacts

1. Secure Outsourcing



2. Privacy Preserving Elicitation of Customer Needs

3. Secure eProcurement



References

1. Chaduvula SC, Atallah MJ, Panchal JH. Secure Co-design: Achieving Optimality without Revealing. *Journal of Computing and Information Science in Engineering*, 2018, In Press, doi: 10.1115/1.4039431
2. Wang, S., Bhandari, S., Chaduvula, S.C., Atallah, M.J., Panchal, J.H. and Ramani, K., 2017. Secure collaboration in engineering systems design. *Journal of Computing and Information Science in Engineering*, *17*(4), p.041010.
3. Sharemind: Bogdanov, D., Niitsoo, M., Toft, T. and Willemson, J., 2012. High-performance secure multi-party computation for data mining applications. *International Journal of Information Security*, *11*(6), pp.403-418.

PURDUE UNIVERSITY Discovery Park

CERIAS