AA. Bibliography

[Genkin 2016] Genkin, D. "ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels." Conference on Computer and Communications Security, August 2016.

[Cauligi 2017] Cauligi, S. "A Flexible, Constant-Time Programming Language." IEEE Secure Development Conference, September 2017.