In the world of “Internet of Things” (IoT), millions of interconnected smart devices have to share information in a fast and secure way. In order to ensure the success and widespread adoption of IoT applications, cryptographic services must be provided to ensure secure communications and avoid skepticism about new emerging technologies. Due to its short key sizes, elliptic curve cryptography is typically deployed on resource-constrained devices in order to enable public-key cryptographic services, i.e. secure key exchanges between smart devices. In the past few years, there has been a growing interest in Curve25519 due to its elegant design aimed at both high-security and high-performance, making it one of the most promising candidates to secure IoT applications. In fact, beside providing appropriate security levels, most IoT applications must adhere to strict latency requirements and provide guarantee to process information in a tiny fraction of time. Until now Curve25519 hardware implementations were
mainly optimized for high-throughput applications, while no special care was given to low-latency designs. In this work, we close this gap and provide a Curve25519 hardware design targeting low-latency applications. Our implementation takes only 13,639 cycles for a variable-base Curve25519 scalar multiplication and can be operated up to 115 MHz on Xilinx Zynq 7030 FPGA devices. This allows to compute a session key in less than 120 μs, which outperforms known FPGA-based Curve25519 implementations by a factor of 2.8, yet requiring 24% less area resources.

Stichworte:  
-ECC, Curve25519, FPGA, Zynq, ECDH, X25519

Dewey Dezimalklassifikation (Liste):  
620 Ingenieurwissenschaften

Kongress- / Buchtitel:  
Euromicro Conference on Digital System Design (DSD 2016)

Kongress / Zusatzinformationen:  
Limassol, Cyprus

Datum der Konferenz:  
08/2016

Jahr:  
2016

Quartal:  
3. Quartal

Jahr / Monat:  
2016-08

Monat:  
Aug

Revied:  
ja

Sprache:  
en

WWW:  

Occurences:  
- Hochschulbibliographie > 2016 > Fakultäten > Elektrotechnik und Informationstechnik > Sicherheit in der Informationstechnik (Prof. Sigl)
  - Einrichtungen > Fakultäten > Fakultät für Elektrotechnik und Informationstechnik > Lehrstühle und Professuren > Sicherheit in der Informationstechnik (Prof. Sigl) > 2016

entries: