(More) Efficient Secure Computation from Garbled Circuits

Yan Huang
David Evans

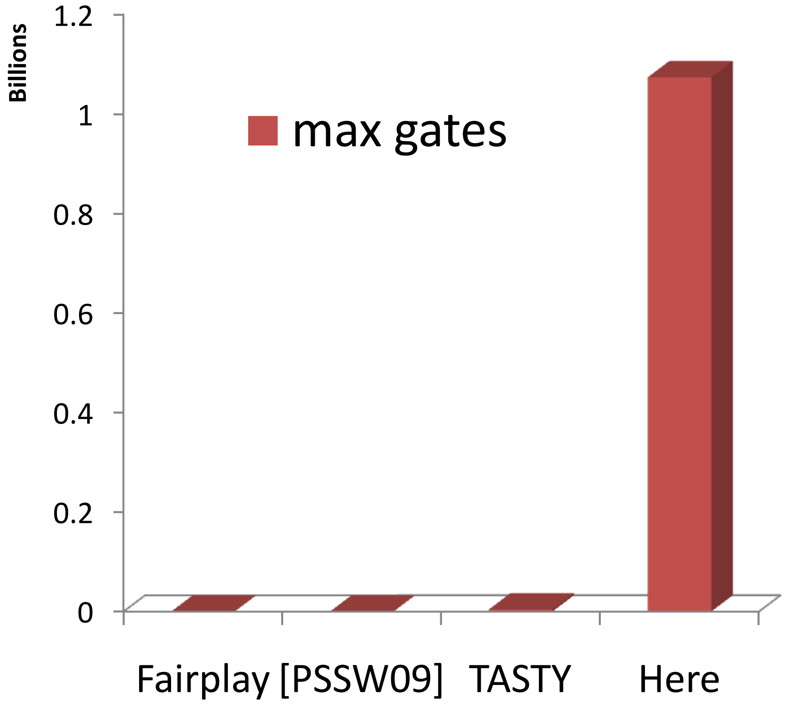
Jonathan Katz
Lior Malka

www.MightBeEvil.com

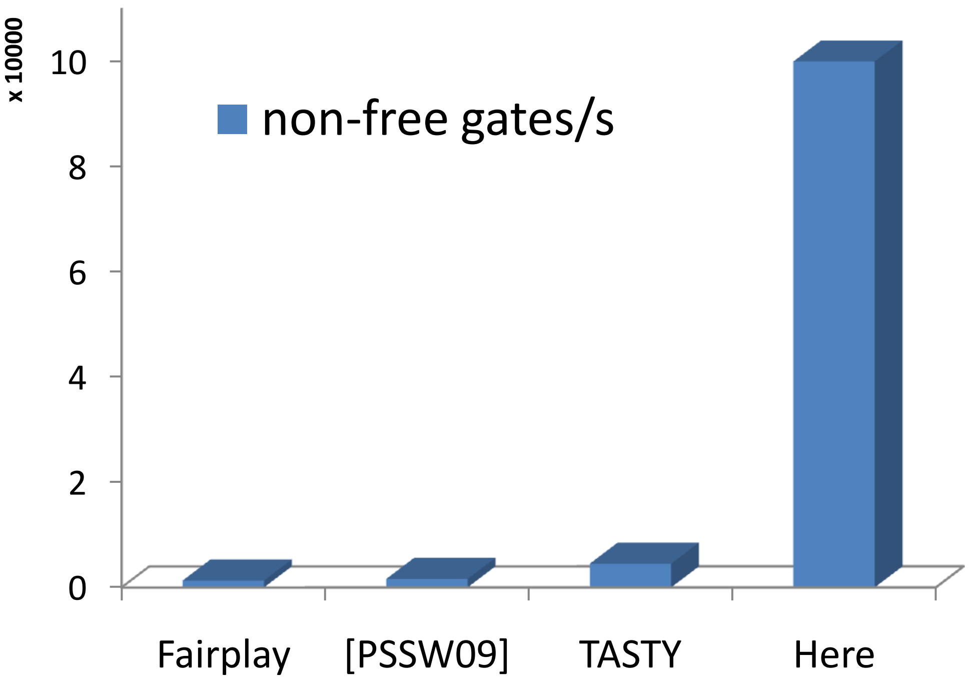
Overview

- A new system for secure 2-party computation that is much more ***scalable*** and significantly ***faster*** than best prior work
- Garbled-circuit protocols can be competitive with "custom" protocols:
  - Hamming distance
  - Private set intersection (PSI)

Our Results

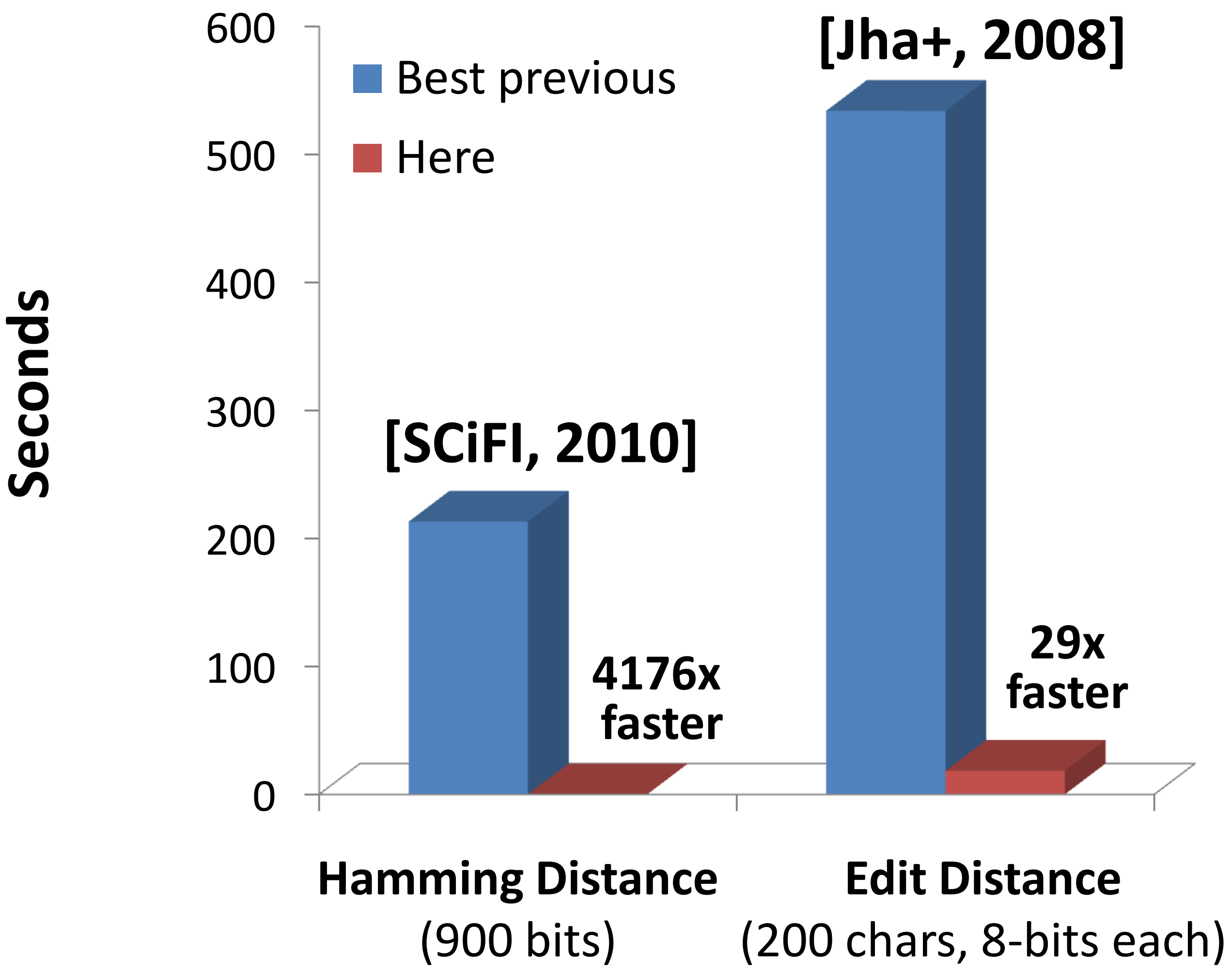


Scalability

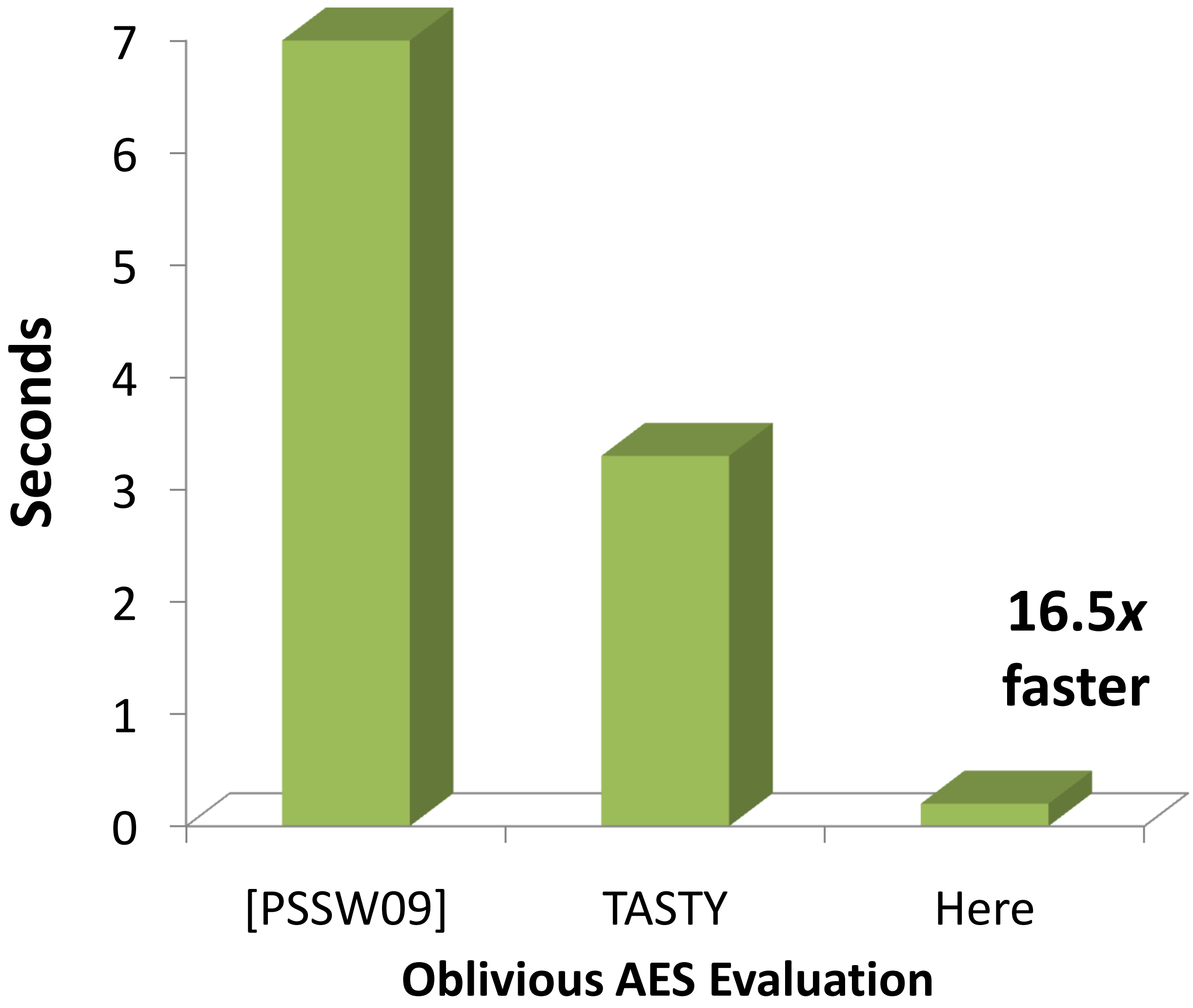


Performance

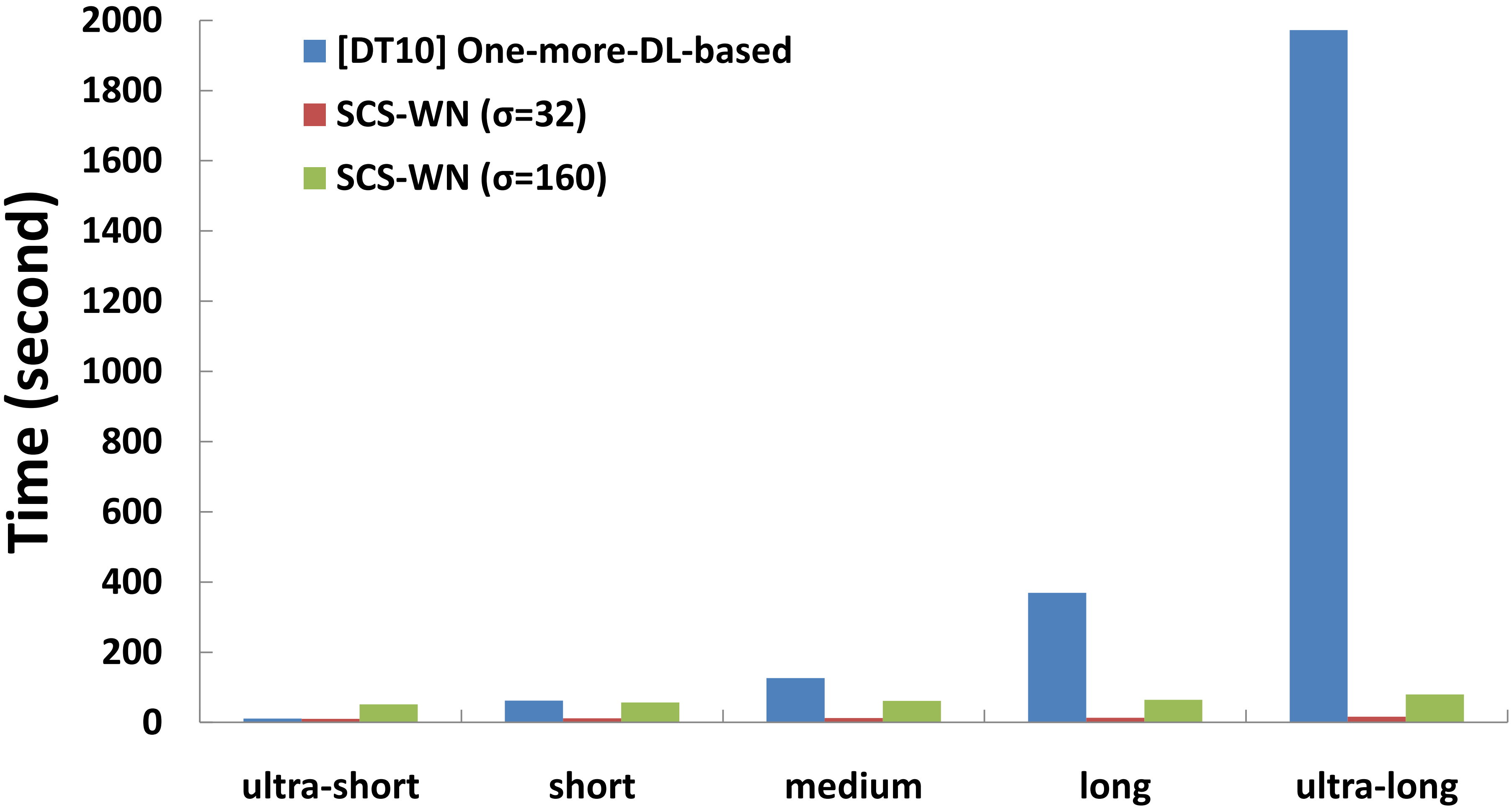
Timing Results



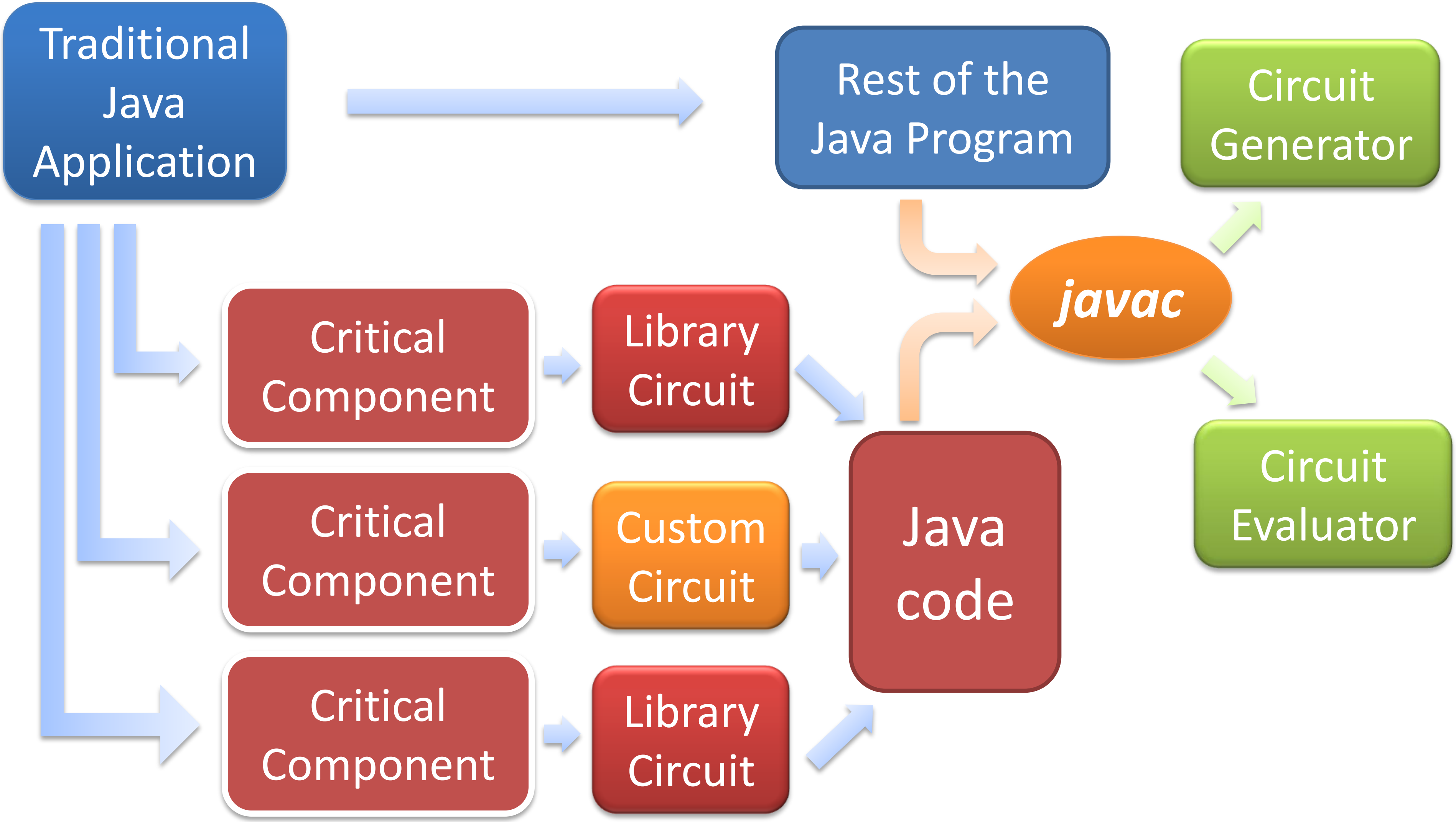
Timing Results



Private Set Intersection



Using the Framework


Traditional Java Application

Rest of the Java Program

Circuit Generator

javac

Critical Component

Library Circuit

Critical Component

Custom Circuit

Java code

Circuit Evaluator

Critical Component

Library Circuit

Thanks!

- "Faster Secure Two-Party Computation Using Garbled Circuits," USENIX Security 2011
- "Private Set Intersection: Are Garbled Circuits Better than Custom Protocols?," In submission

Download framework and Android demo application from **MightBeEvil.com**