Smartphones store highly sensitive information and are the most trusted computing device people own. They offer an ideal platform for privacy-preserving applications.

Oblivious Merging
Oblivious Comparisons
Oblivious Shuffling

Java Program → small adaptation → Adapted Java Program
Security Critical Component f₁ → build Circuit Impl. of f₁
Security Critical Component f₂ → build Circuit Impl. of f₂

Generator (VFM Binary)
Evaluator (VFM Binary)

Oblivious Transfer
Garbled Circuits

public class BITAND {
    Circuit cc;
    public BITAND() {
        cc = AND_1.newInstance();
        cc.build();
    }
    public State execute(State[] s) {
        int L = s.length() / 2;
        State[] result = new State[L];
        for (int i = 0; i < L; i++) {
            State in = s[i].concatenate(s[2 * i], s[2 * i + 1]);
            result[i] = cc.startExecuting(in);
        }
        return result;
    }

Best Papers Opinion
Try our Android app to find which symposium papers you and another person agree are the best.

Common Contacts
Try our Android app to find the common contacts you share with another person without exposing the rest of your contacts.

Collaborators: Jonathan Katz (UMd), SangHyung Koo (UVa), Lior Malka (UMd).
Funding: Air Force Office of Scientific Research (MURI), National Science Foundation, DARPA. Thanks to Google for the Nexus Ones.