Fun things to do with your mobile phone

Peter Schwabe
National Taiwan University

Joint work with Bo-Yin Yang, Shang-Yi Yang

September 30, 2011
CHES 2011 Rump Session, Nara, Japan
Fun things to do with your mobile phone

Android Market

Talking Tom Cat Free
Outfit 7

More from developer
Talking Tom Cat 2 Free
Outfit 7
FREE

Description
Tom is your pet cat, that responds to your touch and repeats everything you say.
PLEASE NOTE: When running the app for the first time you will be required to download additional 3-25 MB to get the best graphics quality for your device.
Fun things to do with your mobile phone

From the description...
“Talking Tom repeats everything you say with a funny voice. You can pet him, poke him, you can even grab his tail. Enjoy hours of fun and laughter with Talking Tom.”
Fun things to do with your mobile phone

---

**droidFart - The #1 Fart Application for Android**

**News**

**It's free!**
posted Jan 9, 2011 7:58 PM by Cory Gibbons

If you were too cheap to buy it for $0.99 before, forget about it! It's now FREE!
Fun things to do with your mobile phone

The Schwartz Unsheathed

Now, it wouldn’t be fair for the iPhone kiddies to be the only ones to have a light saber app, so I decided to give owners of Android devices the opportunity to have some fun as well. Simply touch the saber handle (hit) to engage and disengage the blade. Touch the blade, when out to change the color. When the blade is out, just swing your device around to get those awesome saber swooshing sounds. Swing it hard and abruptly stop to get a saber clash sound. Want a bit more customization? Press the menu button on your device to get a list of available options to play around with.

You can find this app in the Android Market or download it here.

May the Schwartz be with you!
Fun things to do with your mobile phone

The Schwartz Unsheathed

Now it wouldn’t be fair for the iPhone kiddies to be the only ones to have a light saber app, so I decided to give owners of Android devices the opportunity to have some fun as well. Simply touch the saber handle (hit) to engage and disengage the blade. Touch the blade, when out to change the color. When the blade is out, just swing your device around to get those awesome saber swooshing sounds. Swing it hard and abruptly stop to get a saber clash sound. Want a bit more customization? Press the menu button on your device to get a list of available options to play around with.

You can find this app in the Android Market or download it [here].

May the Schwartz be with you!

Admittedly, this one I actually *do* have on my phone
Fun things to do with your mobile phone

▶ Root the phone
▶ Install alternative Android image (thanks to the GAOSP team!)
▶ Install Debian GNU/Linux in a chroot environment
▶ Get access to the cycle counter (thanks to Daniel J. Bernstein!)
▶ Implement and benchmark crypto algorithms in ARM assembly
Fun things to do with your mobile phone

- Root the phone
- Install alternative Android image (thanks to the GAOSP team!)
- Install Debian GNU/Linux in a chroot environment
- Get access to the cycle counter (thanks to Daniel J. Bernstein!)
- Implement and benchmark crypto algorithms in ARM assembly
- For example: SHA-3 candidates
Current status

- Focus on 256-bit versions
- Focus on ARM11 (Qualcomm MSM7200A in my Samsung Galaxy i7500)
- New speed records for 3 out of 5 finalists
- New speed record for SHA-256

- Benchmarks for 4096-bit messages
- JH and Skein are work in progress
  Expect code to appear in eBASH soon
Current status

- Focus on 256-bit versions
- Focus on ARM11 (Qualcomm MSM7200A in my Samsung Galaxy i7500)
- New speed records for 3 out of 5 finalists
- New speed record for SHA-256
- Blake-256 now at 35.63 cycles/byte (before: 47.49 cycles/byte)
- Grøstl-256 now at 114.68 cycles/byte (before: 143.56 cycles/byte)
- Keccak now at 82.80 cycles/byte (before: 101.21 cycles/byte)
- SHA-256 now at 32.31 cycles/byte (before: 40.36 cycles/byte)
- Benchmarks for 4096-bit messages
- JH and Skein are work in progress
  Expect code to appear in eBASH soon
Current status

- Focus on 256-bit versions
- Focus on ARM11 (Qualcomm MSM7200A in my Samsung Galaxy i7500)
- New speed records for 3 out of 5 finalists
- New speed record for SHA-256
- Blake-256 now at 35.63 cycles/byte (before: 47.49 cycles/byte)
- Grøstl-256 now at 114.68 cycles/byte (before: 143.56 cycles/byte)
Current status

- Focus on 256-bit versions
- Focus on ARM11 (Qualcomm MSM7200A in my Samsung Galaxy i7500)
- New speed records for 3 out of 5 finalists
- New speed record for SHA-256
- Blake-256 now at 35.63 cycles/byte (before: 47.49 cycles/byte)
- Grøstl-256 now at 114.68 cycles/byte (before: 143.56 cycles/byte)
- Keccak now at 82.80 cycles/byte (before: 101.21 cycles/byte)
- SHA-256 now at 32.31 cycles/byte (before: 40.36 cycles/byte)
- Benchmarks for 4096-bit messages
- JH and Skein are work in progress
  Expect code to appear in eBASH soon
Current status

- Focus on 256-bit versions
- Focus on ARM11 (Qualcomm MSM7200A in my Samsung Galaxy i7500)
- New speed records for 3 out of 5 finalists
- New speed record for SHA-256
  - Blake-256 now at 35.63 cycles/byte (before: 47.49 cycles/byte)
  - Grøstl-256 now at 114.68 cycles/byte (before: 143.56 cycles/byte)
  - Keccak now at 82.80 cycles/byte (before: 101.21 cycles/byte)
  - SHA-256 now at 32.31 cycles/byte (before: 40.36 cycles/byte)
Current status

- Focus on 256-bit versions
- Focus on ARM11 (Qualcomm MSM7200A in my Samsung Galaxy i7500)
- New speed records for 3 out of 5 finalists
- New speed record for SHA-256
- Blake-256 now at 35.63 cycles/byte (before: 47.49 cycles/byte)
- Grøstl-256 now at 114.68 cycles/byte (before: 143.56 cycles/byte)
- Keccak now at 82.80 cycles/byte (before: 101.21 cycles/byte)
- SHA-256 now at 32.31 cycles/byte (before: 40.36 cycles/byte)
- Benchmarks for 4096-bit messages
- JH and Skein are work in progress
Current status

- Focus on 256-bit versions
- Focus on ARM11 (Qualcomm MSM7200A in my Samsung Galaxy i7500)
- New speed records for 3 out of 5 finalists
- New speed record for SHA-256
- Blake-256 now at 35.63 cycles/byte (before: 47.49 cycles/byte)
- Grøstl-256 now at 114.68 cycles/byte (before: 143.56 cycles/byte)
- Keccak now at 82.80 cycles/byte (before: 101.21 cycles/byte)
- SHA-256 now at 32.31 cycles/byte (before: 40.36 cycles/byte)
- Benchmarks for 4096-bit messages
- JH and Skein are work in progress

Expect code to appear in eBASH soon