

Miroslava Sotáková  
1207 8th Ave, Apt 4L, Brooklyn, NY 11215, USA  
Phone: +1 347 592 3235  
Email: miroslava.sotakova@gmail.com

---

## CURRENT POSITION

- Software engineer at Knewton *September 2012 to present*
- Platform (core and partner-facing products) development in adaptive educational software company
  - Java, Python, AWS, NoSQL (Cassandra), Graph Databases (Titan, proprietary software), Chef Solo, Git, Open Source Technologies
- 

## PAST POSITIONS

- Strategist at Goldman Sachs *November 2010 to January 2012*
- Risk-related application development (backend/frontend)
  - Relational databases (Sybase-IQ, query-optimization, ORM use)
  - Data mining, Reporting
- Postdoc at SUNY Stony Brook *September 2009 to May 2010*
- Position in NSAC (Network Security and Applied Cryptography) lab, Supervisor: Radu Sion
  - Research on efficient ORAM/PIR implementations
- 

## PUBLICATIONS

### Conference

- *On the Power of Two-Party Quantum Cryptography*, with Louis Salvail and Christian Schaffner, ASIACRYPT 2009
- *Learning Low-Density Separators*, with Shai Ben-David, Tyler Lu, and Dávid Pál, AISTATS 2009

### Journal

- *Practical Oblivious Outsourced Storage*, with Peter Williams and Radu Sion, ACM Trans. Inf. Syst. Secur. 14(2): 20 (2011)
- 

## EDUCATION

### PhD, Computer Science

*October 2005 to March 2009*

University of Aarhus, Aarhus, Denmark, GPA: 10.5 (of 12), Thesis title: On the Power of Two-Party Quantum Cryptography, Supervisor: Louis Salvail

### Mgr, Mathematics

*October 2000 – May 2005*

Charles University, Prague, Czech Republic, GPA: 3.96 (of 4), Thesis title: Reversible circuits of small gates, Supervisor: Pavel Pudlák

---

## AWARDS

- Silver medal (78 %) at IMO 2000 (International Math Olympiad), Taejon, Korea
- 2nd prize (69 %) at IMC 2001 (International Math Competition), Prague, Czech Republic
- 2nd prize (61 %) at IMC 2002, Warsaw, Poland
- 6th place (81 %) at Vojtech Jarník International Math Competition 2002, Ostrava, Czech Republic

---

## SKILLS

Programming: Java (Maven, Guice Framework), Python, bash  
Interests: Cryptography and Information Theory, Machine Learning  
Languages: Slovak and Czech (native), English (fluent)  
Personal: Adaptable and quick learner, with strong analytic thinking and mathematical skills.