COMS W6261: Advanced Cryptography: Minimalist Cryptography
Instructor: Tal Malkin

Projects (Evolving Document)

1 Due Dates:

(2/28) General project topic
(3/26) Narrow down what open problem you will work on
(5/02) Submit final project report
(5/03) Project presentations

2 General Advice and Resources

A look at recent cryptography / theory conferences can help to see what's currently being worked on:

1. TCC:
   2015: `http://www.iacr.org/workshops/tcc2015/program.html`
   2016: `http://www.cs.tau.ac.il/conferences/tcc2016/program.html`
2. CRYPTO 2015:
   `https://www.iacr.org/conferences/crypto2015/acceptedpapers.html`
3. EUROCRYPT:
   2015: `https://www.cosic.esat.kuleuven.be/eurocrypt_2015/program.shtml`
   2016: `http://ist.ac.at/eurocrypt2016/`
4. ASIACRYPT 2015:
   `https://www.math.auckland.ac.nz/~sgal018/AC2015/acc.html`
5. Theory conferences: STOC/FOCS and security conferences CCS/ S&P have some crypto papers as well:
   `http://acm-stoc.org/stoc2016/`
   `http://focs15.simons.berkeley.edu/`
   `http://www.sigsac.org/ccs/CCS2015/`
   `http://www.ieee-security.org/TC/SP2015/program.html`
6. The Crypto ePrint (can search recent updates)
   `https://eprint.iacr.org/`
7. Bar-Ilan Winter Schools (including slides and videos):
   2011: Secure Computation and Efficiency
   2012: Lattice-Based Cryptography and Applications
   2013: Bilinear Pairings in Cryptography
   2014: Symmetric Encryption in Theory and in Practice
   2015: Advances in Practical Multiparty Computation
   2015: Cryptography in the Cloud: Verifiable Computation and Special Encryption

8. Simons semester on Crypto `https://simons.berkeley.edu/programs/crypto2015` (see the three workshops, Cryptography Boot Camp, Securing Computation, The Mathematics of Modern Cryptography, as well as the Historical Papers in Cryptography Seminar Series

9. Real World Crypto Conference `http://www.realworldcrypto.com/rwc2016`

In general, any topic related to crypto is fine, including areas such as:
– secure computation (general or specific function classes, reductions and completeness, adaptive GC)
– CCA secure encryption (focusing on efficiency or on minimal assumptions)
– non-malleable codes
– differential privacy
– obfuscation
– functional encryption
– fully homomorphic encryption
– private information retrieval
– cryptographic applications of cryptocurrencies
– delegation and outsourcing
– zero knowledge
– quantum cryptography
– leakage resilient cryptography
– time-lock puzzles, proofs of work, proofs of storage, etc
– connections between cryptography and learning theory
– modern analysis of historical papers in cryptography

3 Specific Suggestions

Here is a list of suggestions for specific topics:

1. Theory / Complexity Oriented:

   Selected specific topics:

   (a) Functional Encryption
   References:

   i. Survey:
   `http://www.di.ens.fr/~wee/pubs/scn14.pdf`

   ii. Function-Private Inner-Product Encryption:
   From bilinear maps: `https://eprint.iacr.org/2015/672.pdf`
   From LWE (but not function-private): `http://eprint.iacr.org/2016/011.pdf`

   iii. Attribute-Based Encryption with Short Public Parameters:
   `http://eprint.iacr.org/2014/754.pdf`

(b) Circuit complexity of WPRF and other cryptographic primitives, or negation complexity of cryptographic primitives

References:

i. See http://www.cs.columbia.edu/~tal/6261/SP16/tal_proposal.pdf for specific suggestions and references that I wrote for these topics.

(c) Basing crypto on P vs NP

References:

i. OWF from NP-hardness implies NP is contained in coAM:
http://eccc.hpi-web.de/report/2014/108/
http://www.wisdom.weizmann.ac.il/~oded/p_aggm.html

ii. PIR from NP-Hardness:
http://eprint.iacr.org/2015/1061.pdf

(d) Private Approximation

References:

i. original paper: Secure Multiparty Computation of Approximations
http://dl.acm.org/citation.cfm?id=1159900

ii. Polylogarithmic Private Approximations and Efficient Matching:
http://researcher.watson.ibm.com/researcher/files/us-dpwoodru/privFin.pdf

iii. Private Approximation of Clustering and Vertex Cover:
https://www.iacr.org/archive/tcc2007/43920382/43920382.pdf

iv. Private Approximation of NP-hard Functions:
http://dl.acm.org/citation.cfm?doid=380752.380850

v. Private Approximation of Search Problems:
http://www.cs.bgu.ac.il/~beimel/Papers/BCNWJournal.pdf

vi. Private Multiparty Sampling and Approximation of Vector Combinations:
http://link.springer.com/chapter/10.1007/978-3-540-73420-8_23

(e) Physical Cryptography

References:

i. Visual Cryptography:
Original paper: http://link.springer.com/chapter/10.1007%2FBFb0053419
Stinson's visual cryptography page (2003): http://cacr.uwaterloo.ca/~dstinson/visual.html
Moire cryptography: http://dl.acm.org/citation.cfm?id=352618

ii. Physical Zero-Knowledge Proofs of Physical Properties:
http://link.springer.com/chapter/10.1007/978-3-662-44381-1_18

iii. Physical Secure Computation:
Secure two-party computation: a visual way: http://eprint.iacr.org/2013/257
Secure Dating with Four or Fewer Cards: https://eprint.iacr.org/2015/1031
Secure Physical Computation using Disposable Circuits: https://eprint.iacr.org/2015/226

(f) Arithmetic Cryptography

References:

i. Original paper:
`https://eprint.iacr.org/2015/336`

(g) Lattice Based Cryptography

References:

i. Survey by Chris Peikert:
`http://web.eecs.umich.edu/~cpeikert/pubs/lattice-survey.pdf`

ii. Learning with Rounding Assumption - could try to prove hard from hardness of LWE:
`http://web.eecs.umich.edu/~cpeikert/pubs/prf-lattice.pdf`
`https://eprint.iacr.org/2013/098`
`https://eprint.iacr.org/2015/769.pdf`

2. Practical Problems

Selected specific topics:

(a) Private Set Intersection (PSI)

Possible specific directions include achieving *fuzzy* PSI (approximate matching), or achieving efficient *sublinear* PSI (which will require a tradeoff with privacy).

References:

i. Practical motivation for sublinear PSI – Moxie Marlinspike's statement of contact discovery problem:
`https://whispersystems.org/blog/contact-discovery/`

ii. Protocols relying on secure equality tests based on OT:

Faster private set intersection based on OT extension:
`https://eprint.iacr.org/2014/447`

Private set intersection using permutation-based hashing.
`https://eprint.iacr.org/2015/634.pdf`

iii. Protocol based on Bloom Filters:

When private set intersection meets big data: an efficient and scalable protocol.
`https://eprint.iacr.org/2013/515.pdf`

iv. Protocol based on general secure two-party computation:

Private set intersection: Are garbled circuits better than custom protocols?
`http://www.cs.virginia.edu/~evans/pubs/ndss2012/psi.pdf`

v. Protocols based on public-key techniques:

Enhancing privacy and trust in electronic communities.
http://www.hpl.hp.com/research/idl/projects/ecommerce/privacy.pdf

Efficient private matching and set intersection.
http://www.pinkas.net/PAPERS/FNP04.pdf

Privacy-preserving set operations.
https://www.iacr.org/archive/crypto2005/36210235/36210235.pdf

Efficient robust private set intersection.
http://www.ece.umd.edu/~danadach/MyPapers/set-int.pdf

Efficient oblivious pseudorandom function with applications to adaptive OT and secure computation of set intersection.
http://www.iacr.org/archive/tcc2009/54440575/54440575.pdf

Practical private set intersection protocols with linear complexity.
https://eprint.iacr.org/2009/491.pdf

Policy-enhanced private set intersection: Sharing information while enforcing privacy policies.
https://eprint.iacr.org/2011/509.pdf

vi. Protocol in server-aided setting for large datasets:
http://research.microsoft.com/en-us/um/people/senyk/pubs/sapsi.pdf

(b) Practical Secure Database Search:
Compare features of these (especially the first two) and try to combine them to get the best parts of each, or try to extend the attacks' applicability and reach.
References:

i. Blind SEER:
http://nsl.cs.columbia.edu/projects/blind_seer/papers/bs_oakland14.pdf
http://nsl.cs.columbia.edu/projects/blind_seer/papers/bs_oakland15.pdf

ii. OSPIR-OXT:
https://eprint.iacr.org/2013/720.pdf

iii. CryptDB:
https://css.csail.mit.edu/cryptdb/

iv. Attacks (mostly on CryptDB):
http://research.microsoft.com/en-us/um/people/senyk/pubs/edb.pdf
http://paul.rutgers.edu/~jasperry/ccs15.pdf

(c) Protocol Analysis:
Take a look at current (or proposed) protocols and analyze them cryptographically (either attacking, proving security properties, or suggesting useful modifications

that improve the scheme in some way – security or functionality or efficiency – while maintaining a cryptographically valid foundation)

References:

i. TLS Security Analysis:
`https://eprint.iacr.org/2013/339.pdf`

ii. Attacks on TLS:
Albrecht-Paterson timing attack (Eurocrypt 16): `https://eprint.iacr.org/2015/1129`
Recent DROWN attack webpage (and paper): `https://drownattack.com`
Recent attacks from miTLS (most recent one is SLOTH): `http://www.mitls.org/pages/attacks`
2014 Kenny Paterson talk slides (TLS starts on p.70): `http://crypto.biu.ac.il/sites/default/files/4th_BIU_Winter_School/Kenny-lecture1-4.pdf`
videos of above talk: `http://crypto.biu.ac.il/attacks-against-record-layers`

iii. Google's certificate transparency proposal
`https://www.certificate-transparency.org/`
`https://datatracker.ietf.org/wg/trans/documents/`
`https://andres.systems/blog/2015-07-22-another-take-at-public-key-distributio`

iv. GIT uses SHA-1 (now known to be weak) for data integrity. Analyze its security (or a theoretical simplified git-variant).
`https://en.wikipedia.org/wiki/SHA-1#Data_integrity`

(d) Bitcoin / blockchain technology:

References:

i. Survey:
`http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf`

ii. Attacks on Mining:
`http://arxiv.org/abs/1311.0243`
`https://eprint.iacr.org/2015/796.pdf`
`http://arxiv.org/abs/1411.7099`

iii. Attacks on Anonymity
`https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf`

iv. Network Attacks:
`http://arxiv.org/abs/1410.6079`

v. Transaction Malleability:
`http://arxiv.org/pdf/1403.6676.pdf`
`https://fc15.ifca.ai/preproceedings/bitcoin/paper_9.pdf`

vi. Hierarchical Keys:
http://link.springer.com/chapter/10.1007/978-3-662-47854-7_31

vii. Analyze on of the variants of the Bitcoin protocol, i.e: the CryptoNote protocol:
http://chainradar.com/xmr/blocks
https://downloads.getmonero.org/whitepaper_annotated.pdf

viii. Bitcoin Workshop
http://fc16.ifca.ai/bitcoin/program.html

ix. Provable Security for Bitcoin:
https://eprint.iacr.org/2014/765
Provable Security for Proof of Work Protocols:
http://eprint.iacr.org/2014/796.pdf

x. Secure multiparty computation with Bitcoin:
http://www.crypto.edu.pl/publications/papers/784.pdf

xi. Using bitcoin in protocol design for fairness:
http://eprint.iacr.org/2014/129.pdf
http://people.csail.mit.edu/ranjit/papers/incentives.pdf

(e) Attacks on Low-Entropy sources of randomness
References:

i. Attacks on PRGs:
http://crypto.di.uoa.gr/CRYPTO.SEC/Randomness_Attacks_files/paper.pdf

ii. Weak key generation from low entropy:
https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final228.pdf

iii. Security analysis of /dev/random:
https://eprint.iacr.org/2013/338.pdf

iv. Security downgrade attack on Diffie-Hellman:
https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf

v. Analysis of backdoored PRGs:
http://www.cs.nyu.edu/~dodis/ps/tprg.pdf

3. Math oriented

Selected specific topics:

(a) Elliptic Curves
References:

i. Pomerance: presentation + open problems
`https://math.dartmouth.edu/~carlp/tatetalk1.pdf`

ii. Elliptic Curves in Practice:
`http://eprint.iacr.org/2013/734.pdf`

(b) Cryptanalysis - choose an assumption/construction and perform cryptanalysis:
References:

i. Candidate: Relativized discrete log assumption:
`http://link.springer.com/chapter/10.1007/11681878_18`

ii. Candidate: Multilinear maps:
`https://eprint.iacr.org/2016/147.pdf`
`https://eprint.iacr.org/2015/934.pdf`
`https://eprint.iacr.org/2014/975.pdf`
`http://eprint.iacr.org/2012/610.pdf`
`https://eprint.iacr.org/2013/183.pdf`