Cryptography and Network Coding

Simon R. Blackburn

Royal Holloway University of London

8th April 2016

Interaction between Cryptography and Network Coding

- Signature schemes to prevent package pollution
- Secret sharing and privacy capacity
- New primitives and cryptanalysis (McEliece analogues)
- Cryptosystems for low-power devices (IoT).

Discrete logarithm problem (DLP)

Let p be a prime and let $g, h \in \mathbb{Z}_p^*$.
Find an integer x (if it exists) such that $h \equiv g^x \mod p$.

In general, this is a hard computational problem (for large p).

Example: Let $p = 11$, $g = 2$ and $h = 9$. Solve the DLP.

x	0	1	2	3	4	5	6	7	8	9
g^x	1	2	4	8	5	10	9	7	3	6

Diffie-Hellman key exchange

Alice and Bob want to agree on a random key K.
They decide upon a large prime p and some $g \in \mathbb{Z}_p^*$, then:

- Alice chooses a random integer $1 \leq a < p-1$ and sends $c_1 = g^a \mod p$ to Bob.
- Bob chooses a random integer $1 \leq b < p-1$ and sends $c_2 = g^b \mod p$ to Alice.
- On receiving c_2 Alice computes $K = c_2^a \mod p$.
- On receiving c_1 Bob computes $K = c_1^b \mod p$.

Alice and Bob both share the same key $K = g^{ab} \mod p$.

It works because $(g^a)^b = (g^b)^a$.

What does security mean?

- An adversary Eve knows p and g, and sees $c_1 = g^a$ and $c_2 = g^b$.
- Eve aims to compute the common key $K = g^{ab}$.
- A minimum level of security: secure if she can't do this.
- If she can solve the DLP, the system is insecure.
- The problem Eve wants to solve is the Diffie–Hellman problem: given c_1 and c_2, compute K.

Ko Lee Cheon Han Kang Park

- Motivation: Diffie–Hellman using non-abelian groups.
- Let G be a (non-abelian) group. For $a, g \in G$ define

$$g^a = a^{-1}ga.$$

- Problem: $(g^a)^b \neq (g^b)^a$, in general.
- Solution: Choose $A \leq G$ and $B \leq G$ with $ab = ba$ for $a \in A$, $b \in B$.
- (A and B are commuting.)
- The analogue of the DLP is the conjugacy search problem: given g and g^a, find a.
- How do you choose a group G and commuting subgroups A and B?
- Ko et al. suggest using a braid group:
  - Easy to represent braids on a computer.
  - Conjugacy search problem seems hard.

The security of Ko *et al.*

- How difficult is the conjugacy search problem?
- There's a nice survey of some of the older work: 'Braid based cryptography' by Patrick Dehornoy.
- Cheon and Jun (2003) gave a (high degree) polynomial-time attack, using representation theory.

The problem with matrix groups (linearisation)

- Let A, B be commuting subgroups of $\mathrm{GL}_n(\mathbb{F}_q)$.
- Let $g \in \mathrm{GL}_n(\mathbb{F}_q)$.
- Eve is given

$$c_1 = a^{-1}ga \text{ for unknown } a \in A \text{ and}$$
$$c_2 = b^{-1}gb \text{ for unknown } b \in B.$$

- She finds invertible $\tilde{a}$ such that

$$\tilde{a}c_1 = g\tilde{a} \text{ and } \tilde{a} \text{ commutes with } B.$$

- Then

$$K = (c_2)^a = (g^a)^b = (g^{\tilde{a}})^b = (g^b)^{\tilde{a}} = c_2^{\tilde{a}}.$$

The Algebraic Eraser

- Proposed by Anshel, Anshel, Goldfeld and Lemieux about 10 years ago.
- Related to the braid group idea.
- Uses the coloured Burau group $\mathrm{GL}(n, \mathbb{F}_q(t_1, \ldots, t_n)) \rtimes \mathrm{Sym}(n)$.
- Elements: (m, σ) where $m \in \mathrm{GL}(n, \mathbb{F}_q(t_1, \ldots, t_n))$ and $\sigma \in \mathrm{Sym}(n)$.
- Product: $(m, \sigma)(m', \sigma') = (m\,(m')^{\sigma}, \sigma\sigma')$.
- G is a subgroup of this group.

The Algebraic Eraser

- There is an action ψ of G on $\mathrm{GL}(n, q) \times \mathrm{Sym}(n)$.
- Choose commuting subgroups A and B of G in some way.
- Choose commuting subgroups C and D of $\mathrm{GL}(n, q)$ in some way.
- Alice picks $c \in C$, $a \in A$ and sends $c_1 = (c, \mathrm{id})\psi(a)$ to Bob.
- Bob picks $d \in D$, $b \in B$ and sends $c_2 = (d, \mathrm{id})\psi(b)$ to Alice.
- Common key is

$$dc_1\psi(b) = cc_2\psi(a) = (cd, \mathrm{id})\psi(ab).$$

History of the security of the Algebraic Eraser 1

- The Algebraic Eraser was made public in 2002.
- January 2008: Myasnikov and Ushakov posted a length-based attack: the parameters were too small.
- May 2011: Gunnells confirms these results, and recommends increasing parameters.
- January 2008 (independently): Kalka, Tsaban and Teicher break the scheme for generic parameters: a (heuristic) linearisation attack to find the secret matrix c, then a (heuristic) permutation group algorithm to find common keys.
- February 2012: Goldfeld and Gunnells show how a careful choice of parameters can avoid this attack.

History of the security of the Algebraic Eraser 2

- July 2015: Sample keys provided to SRB by SecureRF, after request.
- 5 October 2015: SecureRF publish details of a proposed AE standard for ISO.
- 12 October 2015: Ben-Zvi, SRB, Tsaban derive the shared key in under 8 hours (128-bit parameters). SecureRF are informed.
- November 2015: The attack is posted. The BBT attack derives the common key without finding c. Linearisation is used twice: to make membership testing for C easier; and to weaken the information the adversary needs to derive.
- January 2016: Anshel, Atkins, Goldfeld, Gunnells post a response to the attack.
- They sketch how they hope to resist the BBT attack; comment on the security model; say the BBT attack is not always real time.
- February 2016: SRB, Robshaw post a real-time attack on the ISO protocol. Atkins, Goldfeld comment on this.

The future of the Algebraic Eraser?

- "Why Algebraic Eraser may be the riskiest cryptosystem you've never heard of", Dan Goodin, Ars Technica.
- There is a thread on Cryptography Stack Exchange.
- Twitter reaction overwhelmingly negative on AE security.
- I would currently not recommend using the Algebraic Eraser primitive in any applications.
- The only hope: "seems to be to make the problem of expressing a permutation as a short product of given permutations difficult, by working with very carefully chosen distributions."
- The problem: number of braid strands has to be increased to an impractical level.
- Anshel et al propose to use singular matrices to compensate for this.

Some Links

A. Ben-Zvi, S.R. Blackburn and B. Tsaban, 'A practical cryptanalysis of the Algebraic Eraser':

`http://eprint.iacr.org/2015/1102`

Simon R. Blackburn and M.J.B. Robshaw, 'On the Security of the Algebraic Eraser Tag Authentication Protocol':

`http://eprint.iacr.org/2016/091`

See `http://tinyurl.com/oqu2q2b` for an Ars Technica article on this research.