Special Seminar at Bristol in Honour of Clifford Cocks

J.H. Davenport

February 18, 2008

1 Smart

Claims that RSA is not secure, but El-Gamal is. In real life, we don't care about secret keys *per se*, but rather about the message. For example, if the messages are "buy" or "sell", we can determine which is which by observation *if* the encryption algorithm was deterministic. Note that the "RSA problem" is not known to be as hard as factoring. What is the problem that underlies El-Gamal?

The "bad guy" A gets the public key g, $y = g^x$, and two messages $c_1 = g^k$ and $c_2 = my^k$. It has to output m. If this is feasible, it turns out we can solve the Diffie-Hellman problem, so we assume this means El-Gamal is secure.

Shannon's theory by itself is not appropriate, since an "infinitely powerful" adversary can break all public key systems. Hence we get "semantic security" by replacing "infinitely powerful" by "polynomially bounded". Related ot this is "Indistinguishability" (previously known as "polynomial security"). A is given the key, and outputs two messages m_0 and m_1. The challenger then chooses $b \in \{0, 1\}$, and challenges with $E = C_k(m_b)$, and the adversary guesses b'. If $b' = b$ doesn't have probability 0.5, then we don't have indistinguishability. See Goldwasser's thesis (c.1983).

Hence the "Decision Diffie–Hellman" problem: given g^a, g^b and g^c, is $c = ab$? If we can solve El-Gamal, we can solve DDH. In some groups, DDH is definitely easier than DH, whereas in others they are believed to be equivalent.

But how do we represent messages as points on our elliptic curve, and how do we deal with very long messages? We need a Key Encapsulation Mechanism, so we use a block cipher (e.g. AES) keyed by an El-Gamal-like signature based on a hash H of the message. But what about hash functions? Use the Random Oracle Model, in which A can only call H. If we attack this by monitoring the calls to H, we see that$A$ has to call H on the right value. Hence we output one of the calls to H, and its probability of being right is better than random (assuming that A works). What we really wants is IND-CCA-ROM[1]: indistinguishability under chosen-ciphertext attacks in the random oracle model.

[1]There are attacks on SSL treating the SSL server as an encryption algorithm.

This leads to the formulation of the "Gap Diffie–Hellman problem" [not fully explained], which is the abstract problem to which IND-CCA-ROM can be reduced.

Consider $E(\mathbf{F}_p)$, with a bilinear pairing t over E. Then asking whether $t(aP, bP) = t(cP, P)$ can break DDH.

Question: what is Koblitz' objection?

1. The refereeing process (CS is conference-based, not journal-based). Granted it is fast, but in fact success rates are much lower at conferences.

2. Terminology — the theorems state, not "GDH hard ⇒ XXX hard", but rather "GDH hard ⇒ XXX hard in model ZZZ". Hence 'provably secure' is not a valid term. NPS's riposte would be that at least we now have a test for validity of a system.

"It gets rather personal on Oded Goldreich's website!"

2 Clifford Cocks — Recent Developments in Identity Based Public Key

Public Key: Alice sends $E_{PKB}(M)$, having extracted PKB from some PKI, which in practice causes problems.

Shamir 1984: if Bob's public key were his identity, then Alice has no problem, but now Bob has to get his private key from some trusted authority. Equally, we could include items such as date in the public key. Good idea, but no practical implementations for about 15 years.

Pairings Need $E/\mathbf{F}_p$, and a bilinear $e : E \times E \to \mathbf{F}_{p^r}$. Need $|E|$ to divide $p^r - 1$. Boneh & Franklin 2001. The trusted source's secret is some x, and A's secret key is $x \cdot ID_A$. The key of the message is $e(x \cdot ID_A, ID_B) = e(ID_A, x \cdot ID_B)$.

Reciprocity For quadratic recirpocity we need the Legendgre and Jacobi symbols: Jacobi symbols can be computed without being able to factorise. Here (Cocks, 2001) the secret of the Trusted Authority is p, q, and $N = pq$ is published. To send a bit $x = \pm 1$, we choose t such that $(t|N) = x$, and sends $s = t + b/t$ to B. Now $s + 2b = t(1 + b/t)^2$, so $((s+2b)|N) = (t|N) = x$. The problem is that this only sends one bit.

Boneh, Gentry and Hamburg (2007). Given a, b, N we can solve $Ax^2 + By^2 \equiv 1 \pmod N$ *without* factoring N. This is due to Cremona & Rusin 2003. Uses LLL to find suitable small solutions to $Px^2 + Qy^2 = z^2$. Bob and Alice both register and get back the square roots a, b of their public idenities A, B. Each solves $Ax^2 + By^2 = 1$ (need a methodology to ensure they get the same solution!).

$$((ax + by + 1)^2 \equiv 2(ax + 1)(by + 1) \pmod N$$

Then $((ax + 1)|N) = ((by + 1)|N)$ is a shared bit *with no communication*.

Since this is only a shared bit, we need to have multiple such identities $A_1 \ldots$, each with their square roots $a_1 \ldots$. This requires more communication, but *only with the Trusted Authority at initialisation*.

So IDPKC is practicable. Now how do we use it? This is the challenge.

3 Heath-Brown — Counting Solutions of Diophantive Equations

Given $F(x_1, \ldots, x_n) \in \mathbf{Z}[x_1, \ldots, x_n]$. Counts solutions with $|x_i| \leq B$: call this $N_F(B)$. Can build a projective variant. How does $N(B)$ grow as $N \to \infty$. This is linked ot the geometry of $V(F)$ over $\overline{\mathbf{Q}}$.

1. If we can show that $N(B) \to \infty$, then we have proved that there are infintely many solutons!
2. An upper bound for $N_F(B)$ can help solve problems, e.g. Hardy–Littlewood[2] K^*. Choose $F = x_1^d + \cdots x_d^d - x_{d+1}^d - \cdots x_{2d}^d$, and hope $N_F(B) = O(B^\theta$ for any $\theta > d$.
3. Algorithmically, how do we compute $N_F(B)$, or enumerate the solutions.
4. If we want to prove $F = 0$ has no solutions, we can try to prove $N_F(B)$ is small.

If F is homogeneous of degree d, we would naïvely expect $N_F(B) \approx B^{n-d}$, *unless there's a reason why not*. There are many such.

1. $n < d$ gives nonsense.
2. $n = d = 3$ an elliptic curve, so Neron heights gives us $c(\log B)^{r/2}$.
3. $n = 4$, $d = 2$, with $F = x_1^2 + x_2^2 - x_3^2 - x_4^2$ gives $cB^2 \log B$.
4. $n = 4$, $d = 2$, with $F = x_1^2 + x_2^2 + x_3^2 - 7x_4^2$ gives $N_F(B) = 0$.
5. $n = 4$, $d = 3$, with $F = x_1^3 + x_2^3 - x_3^3 - x_4^3$ gives far too many trivial solutions: $\Omega(B^2)$ whereas we expect $O(B^1)$.
6. $n = 3$ $F = x_1 x_2^{d-1} - x_3^d$ gives $\approx B^{2/d}$.
7. $\ldots$

Theorem (Birch 1962) If F is nonsingular with $n > (d-1)2^d$, then $N_F(B) = cB^{n-d} + o(B^{n-d})$. Unfortunately $c = 0$ is sometimes possible, but can often be ruled out.

Inhomogeneous is much harder: Barager has shown that $F = x_1^2 + x_2^2 + x_3^2 + x_4^2 - 4x_1x_2x_3x_4$ has $N_F(B) = (\log B)^{\alpha + o(1)}$ with $\alpha \in [2.3, 2.44]$. So restrict to homogeneous.

[2]Never stated by Hardy–Littlewood: due to Hooley!

Define 'trivial' to be solutions on a straight line in the surface. Let N_1 be N excluding such solutions. Then Manin's conjecture is $N_1(B) = cB(\log B)^{p-1}\{1+o(1)\}$, where p is the rank of $\mathrm{Pic}(V)$. This has been proved for some special cases: $x_1x_2x_3 = x_4^3$ for example, but it is not yet known for any non-singular surface.

For $n = 4$, $d \geq 3$, then $N_1(B) = O(B^\theta)$ with $\theta < 2$. This means that trivial solutions dominate non-trivial ones.

More generally, for $n = 4$, there are finitely many curves of degree $\leq d-2$, and these may contribute "trivial" solutons, so define N_2 to exclude these as well. Example: $F = (x_1x_2^2 - x_3^3)G + x_4H$ is trivial for all $(a^3, b^3, ab^2, 0)$. Then (Heath-Brown, Salberger) $N_2(B) << B^\theta$ for $\theta > 3/\sqrt{d}$. Compare Bombieri–Lang conjecture.

Consider $F = f(x_1, x_2) - f(x_3, x_4)$, so we are looking at numbers represented by f in more than one way. Then for $d \geq 3$, $N_1 \sim cB^{2/d}$ whereas $N_2 = o(B^{2/d})$.

Consider $\Sigma_{i=1}^r a_i x_i^d$. Let $S(d) = \Sigma_{-B \leq x \leq B} \exp(2\pi i \alpha x^d)$. Then

$$N(B) = \int_o^1 S(a_1\alpha \dots S(a_r\alpha) d\alpha.$$

Have a usual "major/minor arcs" issue. [I got lost here.] Claims that this shows that analytic methods can do things that geometry cannot.

De la Bretèche *et al.* studied $x_1x_2^2 + x_2x_3^2 + x_4^3 = 0$. Geometry can map this to the" universal torsor", and we then use analytic methods.

4 Hugh Montgomery

[Not a formal talk, but I bumped into him at the reception. It turns out he's over at Heilbronn for a year, and he's giving a talk at this year's BMC: "Cambridge forty years ago".]

He described the following theorem of Conway, which I hope I have captured correctly. Let $\pi : \mathbf{N} \to \mathbf{N}$ be a permutation. Then it is claimed that the following two properties are equivalent.

1. For all sequences s_i, $\Sigma_{i=0}^\infty s_i$ converges implies $\Sigma_{i=0}^\infty s_{\pi(i)}$ converges.
2. $\exists B\ \forall N\ \pi^{-1}[0 \dots N]$ consists of at most B blocks.

[I hope I've got the theorem down right: it's hard to do when the theorem was described to one an hour previously over canapés.]

Note that the second property can be true of π but not π^{-1}. From memory (his, and then mine) Conway's example was as follows: $\pi(0) = 0$; $\pi(1) = 1$; $\pi(2, 3, 4) = (3, 2, 4)$; $\pi(5, 6, 7, 8, 9) = (7, 6, 8, 5, 9)$ and so on for each $(n^2, (n+1)^2]$.

Does anyone have a reference to this theorem?