Elliptic Curve Cryptography

This is not in Bach's notes, but ECC has become so important lately that it would be remiss to omit it. The main reason for its success is that there are no known attacks in the general case that take fewer than about $\sqrt{p}$ operations (which Baby-Step Giant-Step takes). This makes ECC more suitable in constrained environments, where long key-lengths are infeasible. NSA tells us that 1024-bit RSA is equivalent to 160-bit ECC; 2048-bit RSA to 224-bit ECC; 3072-bit RSA to 256-bit ECC. There are elliptic curves in the FIPS 186-3 standards defined over $\mathbf{Z}_p$ where p has $192, 224, 256, 384$, and 521 bits.

Elliptic Curves over $\mathbf{Z}_p$: Consider the curve $y^2 = f(x)$, where f is a cubic polynomial with coefficients in $\mathbf{Z}_p$ (p a large prime) such that f has no repeated roots. A point on the curve is either a pair (x, y) of elements of $\mathbf{Z}_p$ that satisfies $y^2 = f(x)$ (computed using modular arithmetic in $\mathbf{Z}_p$) or the point at infinity ∞. Hasse's theorem says that the number of points on the curve lies between $p+1-2\sqrt{p}$ and $p+1+2\sqrt{p}$, so there are about p points on the curve.

Addition of Points: To add two typical points P, Q on the curve, find the third point of intersection of the line joining P to Q and then reflect it in the x-axis to obtain $P + Q$. If $P = Q$, do the same with the tangent line at P. If the line joining P to Q does not intersect the curve in a third point, then set $P + Q = \infty$. Set $P + \infty = P$ for any P. This defines an addition law that is commutative and associative, so makes $nP = P + ... + P$ (n times) well-defined for any positive integer n and point P on the curve.

Formulae: For quick implementation, suppose the curve is $y^2 = x^3 + ax + b$ and $P = (x_1, y_1), Q = (x_2, y_2)$. Then $P + Q = (x_3, y_3)$, where if we set $s = (y_2 - y_1)/(x_2 - x_1)$ (for $P \neq Q$) and $s = (3x_1^2 + a)/(2y_1)$ (for $P = Q$), then $x_3 = s^2 - x_1 - x_2$ and $y_3 = s(x_1 - x_3) - y_1$. Note that this includes the case where $x_1 = x_2$ but $y_1 \neq y_2$. In that case s is undefined and we set $P + Q = \infty$.

Elliptic Curve Diffie-Hellman protocol (ECDH): Alice and Bob agree on a curve E and a point P on that curve (perhaps using one from the standards). Alice and Bob separately pick secret positive integers a, b. Alice sends aP to Bob and Bob sends bP to Alice. (Note that each can be computed quickly using doubling and adding.) They can each compute $(ab)P$ and use that to produce a shared key for a private-key cryptosystem.

Elliptic Curve Discrete Log Problem (ECDLP): The problem an eavesdropper faces is: given p, E, P, aP, find a.

Baby-Step Giant-Step (BSGS): Pick $m > \sqrt{\#E}$. Suppose $Q = xP$ is intercepted and write $x = x_0 + x_1 m$. Compute two lists of points. First list (baby steps): $x_0 P$ for $x_0 = 0, 1, ..., m-1$. Second list (giant steps): $Q + x_1(-mP)$ for $x_1 = 0, 1, ..., m-1$. Sort and match. If $Q + x_1(-mP) = x_0 P$, then $Q = (x_0 + x_1 m)P$ and we've solved for x. (Takes about $\sqrt{p}$ operations.)