ECOH: the Elliptic Curve Only Hash

Presentation to the First SHA-3 Candidate Conference

Daniel R. L. Brown

Certicom Research

K. U. Leuven, Belgium
February 26, 2009

Parameters

Hash	n	E and G	m	$blen$	$ilen$	$clen$
ECOH-224	224	B-283	283	128	64	64
ECOH-256	256	B-283	283	128	64	64
ECOH-384	384	B-409	409	192	64	64
ECOH-512	512	B-571	571	256	128	128

Pseudocode

1. Pad & parse: $M\|1\|0^j = N_0\| \ldots \|N_{k-1}$ ($blen$-bit blocks).
2. Index: $O_i = N_i\|I_i$ ($ilen$-bit integer i).
3. Tail: $O_k = (\bigoplus_{i=0}^{k-1} N_i)\|I_{mlen}$ ($|M| = mlen$).
4. Search: $X_i = (0^{m-(blen+ilen+clen)}\|O_i\|0^{clen}) \oplus C_i$ where C_i smallest integer making X_i valid x-coordinate.
5. Expand: $P_i = (x_i, y_i)$ where $(y_i/x_i)[m-1] = N_i[0]$.
6. Add: $Q = \sum_{i=0}^{k} P_i$.
7. Finalize: $\lfloor x(Q + \lfloor x(Q)/2 \rfloor G)/2 \rfloor \bmod 2^n$.

certicom

Generalizations

1. Different curves.
   - Slightly larger curves faster.
   - Special curves halves number of x's to try.
2. Encrypt or hash each block:
   - Easier proofs, under ideal assumptions.
   - Seems to thwart Semaev attacks.
3. Obfuscate the tail: possibly thwarts some attacks.
4. Modified finalization: may reduce distinguishability.

certicom

Heuristic Security Analysis

1. Bellare and Miccancio's *MuHASH*, 1997, minus pre-existing hash function, plus finalization.
2. Wagner's generalized birthday attack for second preimages: appears to be thwarted by checksum tail.
3. Semaev polynomials: solving implies collision, but may be hard since related to ECDLP.
4. Wagner and Dai's k-sum problem, hard as ECDLP.
5. Shifted log problem: hard as ECDSA.
6. Generic groups: shifted log hard, collisions hard.
7. Pseudorandomness: ECOH outputs distinguishable as ECOH outputs. Do not use for stream cipher, otherwise ok.

certicom

Efficiency

1. Optimized 32-bit implementation relatively slow:
   7.5, 10, 11.5 kcpb for 224/256, 384, 512, respectively.
2. Potential 25x faster with
   Carryless multiplies (e.g. Intel AVX) for binary field arithmetic
   Simultaneous inversion (inverse replaced with three times).
3. Parallelism ...
4. Incrementalism ... with negligible memory cost.
5. Synergy with other ECC.

certicom