Report on Present State of ECDSA Evaluation (full evaluation)

January 28, 2002

Atsushi Shimbo, Member

Public-Key Cryptography Subcommittee

ECDSA

- Category: Signature
- Security basis: Discrete logarithm problem on elliptic curves
- Provable security: No established provable security
  (no proof with random oracle model)
  There are results from Brown using a generic group model
- Characteristics (compared to RSA signature)
  - Key length is short
  - Signature is small
  - Signature generation time is short
- SW implementation information (ECDSA in SEC1 submitter):
  Key generation: 1.9ms, signature generation: 3.7ms,
  signature verification: 9.7ms (Pentium III 650MHz)

ECDSA specifications

- There were two schemes evaluated in CRYPTREC2001:
  - ECDSA in SEC1: Submission from CRYPTREC2000
  - ANSI X9.62: one of the signature systems included in guidelines for electronic signature law
- Same signature scheme
- Differences in recommended elliptic curves
  - SEC1: Recommends Koblitz curves as well as random curves
    Parameter a is fixed with nearly all curves
  - ANSI: Presents random curves as well as curves generated by the Weil method as samples
    Curve parameter a is also random

Full evaluation

- Four evaluators were requested to evaluate the scheme based on the following perspectives:
  - Cryptographic scheme
    - Verification of provable security in generic group model
  - Cryptographic primitives
    - Verification of security of Koblitz curves (ECDSA in SEC1)
  - Other issues and comments
    - Evaluation of security from any desired perspective

Brown's paper

- Security proof for generic DSA using generic group model

  [Generic DSA] ECDSA is generalized to signature schemes using (additive) groups of any prime order.

  [Generic group model] Virtual model assuming that group element expressions are randomly provided.

  – Bijections σ for bit sequence set S are randomly provided from additive group Z_n with prime order n.

  – Group operations are performed using queries to the generic group oracle determining σ.

- [Main theorem] If there exists a forger performing existential forgery using adaptive chosen message attacks, then it is possible to construct an algorithm for determining hash function collisions.

Evaluation comments
– Provable security –

- Brown's theorem is generally correct
  - An evaluator provided a separate proof, correcting the algorithm's success probability and execution time.
  - An evaluator noted that the description of Brown's proof was insufficient (incomplete).
- Significance of proof using generic group model
  - The model has a shorter history than the random oracle model, so the real significance of the proof is more limited.
  - Some evaluators gave fairly positive evaluations while others did not.
    - The current ECDLP solution is a generic model type in which group operations are black-boxed, so this is an indicator of security against the attacks.
    - With ECDSA, group element expressions cannot be considered generic, and specific attacks against ECDSA cannot be explained.

Evaluation comments

– Security of Koblitz curves –

- With Koblitz curves, there are techniques that provide a slight speed increase to the rho method, which is the ECDLP solution.

  [Wiener etc.][Gallant etc.]

  – Solved at a speed $\sqrt{2m}$ times as fast with a curve on F_{2^m} .

  (approximately 16 times as fast with m=160)

  – Can be handled by slightly increasing the parameter size.

- Some evaluators were concerned about the possibility that a special attack would be discovered.

Evaluation comments

– Pseudo-random number generators –

- Care must be taken in considering the pseudo-random number generators presented in ANSI X9.62.
  - Bleichenbacher attack on DSA[FIPS 186]

    k=rand mod n not distributed uniformly over [1,n-1]
    - Some evaluators recommended corrections similar to FIPS186-2 (+change notice 1).
- Examples of attacks on DSA implementations using weak pseudo-random number generators based on linear congruence method [Bellare etc.]

Evaluation comments

– Verification of elliptic curve parameters –

- Some evaluators felt the elliptic curve parameters should permit verification that there are no trapdoors.
  - Curves and base points G are not limited, even when using “verifiable curve generation”.
  - It was recommended that the asymmetric-key proof include definition field Fq, seed, a, b, base point G, order n, and asymmetric key Y in their entirety.
  - In addition, it was recommended that a reliable third-party organization be established to verify the elliptic curve parameters.