On the generation of one-time keys in DL signature schemes

Daniel Bleichenbacher

Bell Labs, Lucent Technologies

Nov 15, 2000

Overview

- DSA/ Notation
- Proposed randomizers for one-time keys
- Bias of one-time key generation
- Previous results
- New results
- Conclusion

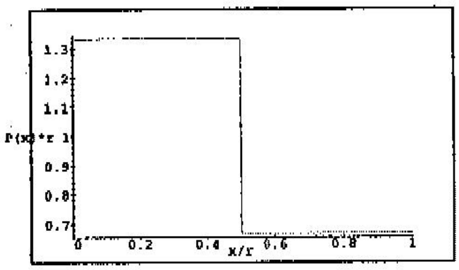
DSA (Notation)

- Domain parameters: q, g, r,
  where g is generator of order r in GF(q).
- Private key: $0<s<r$.
- Public key: $w=g^x \bmod q$
- Message: M_j
- Signature generation:
  generate one-time key (u_j, v_j=exp(g, u_j) mod q)
  convert u_j into c_j using FE2IP
  compute $d_j=u_j^{-1}(\mathrm{h}(M_j)+sc_j) \bmod q$
  then (c_j, d_j) is the signature of M_j

One-time key generation (simplified)

- Pseudorandom function
  $G:\{0,1\}^{320} \rightarrow \{0,1\}^{160}$.
- State j of PRNG: t_j, KKEY$_j$
- Generation:
  convert G(t_j,KKEY$_j$) into integer i_j,
  compute $u_j = i_j \bmod r$
  compute $v_j = \exp(g, u_j) \bmod p$
  update t_j and KKEY$_j$
  return (u_j, v_j)

Distribution of one-time secret u_j



Because of G(t,KKEY) mod r values in the interval $[0, 2^{160}-r-1]$ are twice as likely as values in the interval $[2^{160}-r, r-1]$.

Previous work

Problem: Given partial information about the one-time keys u_j, Can the DSA secret key be found?

- Frieze et al. [1988] : general system of eqns.
- Boneh and Venkatesan [1996] : $\Omega(\log(r))$ bits of u_j must be known.
- Howgrave-Graham and Smart [1999]: 8 bits of u_j must be known.
- Nguyen and Shparlinski [2000]: 3 bits of u_j must be known.

New result

- New *heuristic* algorithm for finding the DSA private key s.
- If $r \sim 0.7 * 2^{160}$, then s can be found with
  2^{22} known signatures,
  2^{41} memory,
  2^{64} time.
- Trade-offs between known signatures, memory and time are possible.
- No *real* experiments so far.

Definition of bias

- Let **X** be a random variable with probability distribution $P_X(x)$ then

$$\text{bias}(\mathbf{X}) = \sum_x P_X(x) e^{2\pi i x / r}$$

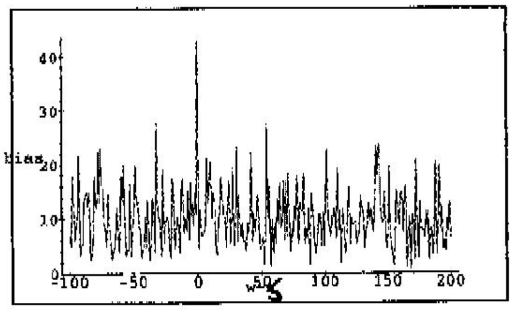
Let $Y=(y_1,\ldots,y_L)$ be an array, then

$$\text{bias}(Y) = \frac{1}{L}\sum_{j=1}^{L} e^{2\pi i y_j / r}$$

Idea 1: Distinguishing good guesses from wrong guesses.

- Let (c_j, d_j, M_j) for $1 <= j <= L$ be DSA signatures
- Let $f_j = c_j d_j^{-1} \bmod r$
  and $h_j = \mathrm{h}(M_j)\, d_j^{-1} \bmod r$
- Define $\mathrm{B}(w) = (h_1 + f_1 w, \ldots, h_L + f_L w)$
- Then $\mathrm{B}(s) = (u_1, \ldots, u_L)$ and hence is biased.
- But $|\mathrm{bias}(\mathrm{B}(w))|$ for $w \neq s$ is small.

Small example: Bias

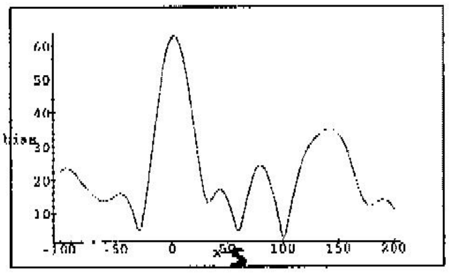


$|\mathrm{bias}(\mathrm{B}(w))|$ for $w = s-100, \ldots, s+100$
$\Rightarrow$ peak for $w = s$

Idea 2: Collision search

- Given (f_j, h_j) for $1 <= j <= L$, find
  $f'_j = f_{j1} + \ldots + f_{jR}$
  $h'_j = h_{j1} + \ldots + h_{jR}$,
  such that f'_j is in a small interval [1,C].
- $\Rightarrow$ bias(B'(s)) ~ bias(B(s))^R.
- $\Rightarrow$ |bias(B'(w))| is large if $|w-s| \ll r/C$

Bias after collision search



|bias(B'(w))| for $w = s-100, \ldots, s+200$ after collision search with $C=r/32$ and $R=2$
$\Rightarrow$ peak around s becomes wide.
$\Rightarrow$ Compute |bias(B'(w))| for O(C) values only.

More ideas:

- Use an idea by Shamir and Schroeppel [1981] to save memory in the collision search.
- Use FFT to compute |bias(B'(w))| efficiently.
- Use CRT and Pollard-lambda for finding the missing bits of s.
- *etc.*

Conclusion: IEEE P1363

- p.198, note 7:
  "The private key should be generated at random from the range [1,r-1], because this maximizes the difficulty of recovering the private key by collision-search methods. A desired level of security can also be provided when the private key is restricted to a large enough subset of the range, e.g. is shorter than the subgroup order, has low weight or has some other structure. Such choices require further security analysis by the implementer ..."
- ⇒ This recommendation is not sufficient.

Conclusion: IEEE P1363a/D6

- The methods proposed in A.16.14 and A.16.15 are biased and should be replaced.
- My recommendation:
  Require that one-time keys are either chosen uniformly at random in a way that is not distinguishable from a uniform distribution in [1,r-1].