



The Insecurity of the Digital Signature Algorithm with Partially Known Nonces

BOOKS
SURVEYS
JOURNALS
CONFERENCES
VULGARISATION
MISC

- **Download:** [In *J. of Cryptology*, Vol. 15, Number 3, Pages 151-176, 2002 \(.gz version\)](#)
- **Authors:** [Phong Q. Nguyen](#) and [Igor E. Shparlinski](#)
- *Journal of Cryptology, Volume 15 (2002), pp 151--176.*

- **Abstract:** We present a polynomial-time algorithm that provably recovers the signer's secret DSA key when a few consecutive bits of the random nonces k (used at each signature generation) are known for a number of DSA signatures at most linear in $\log q$ (q denoting as usual the small prime of DSA), under a reasonable assumption on the hash function used in DSA. For most significant or least significant bits, the number of required bits is about $\log^{1/2} q$, but can be decreased to $\log \log q$ with a running time $q^{O(1/\log \log q)}$ subexponential in $\log q$, and even further to 2 in polynomial time if one assumes access to ideal lattice basis reduction, namely an oracle for the lattice closest vector problem for the infinity norm. For arbitrary consecutive bits, the attack requires twice as many bits. All previously known results were only heuristic, including those of Howgrave-Graham and Smart who recently introduced that topic. Our attack is based on a connection with the *hidden number problem* (HNP) introduced at Crypto~'96 by Boneh and Venkatesan in order to study the bit-security of the Diffie-Hellman key exchange. The HNP consists, given a prime number q , of recovering a number $\alpha \in \mathbb{F}_q$ such that for many known random $t \in \mathbb{F}_q$ a certain approximation of $t \alpha$ is known. To handle the DSA case, we extend Boneh and Venkatesan's results on the HNP to the case where t has not necessarily perfectly uniform distribution, and establish uniformity statements on the DSA signatures, using exponential sum techniques. The efficiency of our attack has been validated experimentally, and illustrates once again the fact that one should be very cautious with the pseudo-random generation of the nonce within DSA.