The art of cryptography, summer 2013

Lattices and cryptography

Prof. Dr. Joachim von zur Gathen
Dr. Daniel Loebenberger

We recall the Diffie-Hellman problem (DH_G): we have a cyclic group $G = \langle g \rangle$ with generator g, are given $A = g^a$ and $B = g^b$ (but do not know the exponents a and b), and have to compute g^{ab}. Then (g^a, g^b, g^{ab}) are a DH triple.
For $G = \mathbb{Z}_p^\times$, we need a prime p of about 2000 bits at current security requirements. In many applications, only a small part of the common key is used, say the leading 256 bits as a shared AES key. We proceed to show that the leading $5 \cdot \sqrt{2000} \approx 224$ bits are secure.

Algorithm 1. Reduction from DH to leading bits of DH.

Input: A prime p, a generator g of $\mathbb{Z}_p^\times$, and A, $B \in \mathbb{Z}_p^\times$.
Output: Some $w \in \mathbb{Z}_p^\times$, likely to solve the DH problem for A, B.

1. $\lambda \longleftarrow (\log_2 p)^{1/2}$,
   $\mu \longleftarrow 5\lambda$,
   $\alpha = \lceil 2^\mu \rceil$,
   $n \longleftarrow \lfloor \lambda/2 \rfloor$.
2. $r \overset{\text{⚂⚄}}{\longleftarrow} \mathbb{Z}_{p-1}$,
   $C \longleftarrow Ag^r$.
3. For $1 \leq i \leq n$ do steps 4 and 5.
4. $\qquad d_i \overset{\text{⚂⚄}}{\longleftarrow} \mathbb{Z}_{p-1}$, $D_i \longleftarrow Bg^{d_i}$, $t_i \longleftarrow C^{d_i}$.
5. $\qquad$ Call a leading bit algorithm for C and D_i to return $u_i \in V_\alpha(y_i \text{ srem } p)$, where (C, D_i, y_i) is a DH triple.
6. Call the hidden number algorithm with input $t = (t_1, \ldots, t_n)$ and $u = (u_1, \ldots, u_n)$ to return $s \in \mathbb{Z}_p^\times$ or "failure". In the latter case return "failure".
7. Return $w = sB^{-r} \in \mathbb{Z}_p^\times$.

THEOREM 2. *Let $p \geq 2^{36}$ be a k-bit prime and $G = \mathbb{Z}_p^{\times}$. The output s of the algorithm solves the DH_G problem for A, B with probability at least $1/(4 \log_2 k)$. It uses polynomial time plus at most $\sqrt{k}/2$ calls to a leading bit algorithm for DH_G.*

Corollary 3. *Let* $p \geq 2^{36}$ *be a* k*-bit prime,* $G = \mathbb{Z}_p^\times$*, and* $\alpha = \lceil 2^{5\sqrt{k}} \rceil$*. If* DH_G *is secure against polynomial-time attacks with success probability at least* $1 - 1/(4 \log_2 k)$*, then* DH_G *is also secure against polynomial-time* α*-approximations.*