A remark on the efficiency of identification schemes

Mike Burmester
RHBNC - University of London
Egham, Surrey TW20 OEX
U.K.

Abstract

The efficiency parameters of identification schemes (memory size, communication cost, computational complexity) are based on given security levels and should allow for the 'worst-case' probability of error (forgery). We consider instances of the schemes in [OO88] and [Sch90] for which the efficiency is not as good as claimed.

Introduction. Ohta-Okamoto presented [OO88] a modification of the Fiat-Shamir [FS86] identification scheme which claims to reduce the probability of error (forgery) from 2^{-kt} to L^{-kt} (for suitable L). Here k is the number of secret information integers, t the number of iterations and L the exponent (for the Fiat-Shamir scheme $L = 2$). We shall see that this is not always true, *e.g.,* there are instances for which this probability is 2^{-kt} and indeed 2^{-t}, if we use the argument in [BD89]. In particular, for the parallel implementation the probability of error can be $1/2$. Similar instances occur with the scheme in [Sch90].

The schemes that we consider are based on interactive proof systems. A formal setting for such systems is given in [GMR89,FFS88]. Let A be the prover, B the verifier and (A, B) an interactive proof of membership in a language $\mathcal{L}$. For every dishonest prover $\tilde{A}$ there is a probability that B will accept when the input $x \notin \mathcal{L}$. The probability of error of (A, B) is the largest such probability, taken over all $\tilde{A}$. This is negligible when the proof (A, B) is sound [GMR89]. The probability of error for proofs of knowledge [FFS88] is defined in a similar way.

The Ohta-Okamoto scheme. Let $n = pq$, p and q distinct odd primes, $L \geq 2$, and $x = (I\,; n, L)$, $1 < I < n$, be the input. The prover A proves that there exists (or that it knows) an S such that $I = S^L \bmod n$. The protocol has four steps which are repeated $t = O(\log n)$ times. In Step 1, A sends B the number $X = R^L \bmod n$, R random in Z_n. In Step 2, B sends A a random query $E \in Z_L$ and in Step 3, A replies with $Y = R \cdot S^E \bmod n$. Finally in Step 4, B verifies that $Y^L \equiv X \cdot I^E \pmod n$. B accepts (the proof of A) if the verification is valid for all t iterations.

We shall show that the probability of error can be as large as 2^{-t}. Suppose that $L = 2L_1$, L_1 odd, and that $I, S_1 \in Z_n^*$ are such that $I = S_1^{L_1} \bmod n$ with S_1 a quadratic

I.B. Damgard (Ed.): Advances in Cryptology - EUROCRYPT '90, LNCS 473, pp. 493-495, 1991.

non-residue $\bmod n$. Then I is a non-residue and does not have an L-th root $\bmod n$. Let $\tilde{A}$ be a dishonest prover which guesses the parity of the queries randomly, with uniform distribution. In Step 1, $\tilde{A}$ sends $X = R^L \bmod n$ if the guessed parity is even, and $X = R^L \cdot I^{-1} \bmod n$ if the guessed parity is odd. In Step 3, $\tilde{A}$ sends $Y = R \cdot S_1^{E/2} \bmod n$ if the (actual) query E is even, and $Y = R \cdot S_1^{(E-1)/2} \bmod n$ if E is odd. Then B will accept when $\tilde{A}$ has guessed the parity correctly. Indeed for E even, $X \cdot I^E \equiv R^L \cdot S_1^{L_1 E} \equiv (R \cdot S_1^{E/2})^L \equiv Y^L \pmod n$ and for E odd, $X \cdot I^E \equiv R^L \cdot I^{-1} \cdot S_1^{L_1 E} \equiv R^L \cdot S_1^{L_1(E-1)} \equiv (R \cdot S_1^{(E-1)/2})^L \equiv Y^L \pmod n$. So B will accept with probability $1/2$ for each iteration. Therefore the probability of error for the proof (A, B) is at least 2^{-t}.

A similar example can be used with proofs of knowledge. For 'unrestricted input' proofs the input I has to be an L-th root. Again we take $L = 2L_1$, only this time L_1 need not be odd and S_1 is a quadratic residue. The dishonest prover $\tilde{A}$ is given on its knowledge tape S_1 but not $\sqrt{S_1} \bmod n$ (the soundness condition for proofs of knowledge [FFS88] does not restrict the contents of the knowledge tape of $\tilde{A}$: we assume that it is hard to compute $\sqrt{S_1} \bmod n$, given S_1). So $\tilde{A}$ does not *know* an L-th root of I. As before, if $\tilde{A}$ guesses the parities then B will accept with probability 2^{-t}.

This argument can be easily extended to other values of L which have a common factor with $p-1$ or $q-1$. An illustration of a more general case for which n is a product of three primes and L is a prime is given in [BD89].

In [OO88, p.241] it is argued that the probability of cheating is $1/L$ when $t = 1$ and L is the product of distinct primes with $(L, p-1) = L$, provided that there is no probabilistic polynomial time algorithm for factoring. This is not true for our example. For us, with such $L > 2$, L even, the probability of error is $1/2$, and there is no reason why factoring should be any easier (*e.g.*, when S_1 is a quadratic non-residue, for proofs of membership, or when $\tilde{A}$ has S_1 on its knowledge tape, for proofs of knowledge).

In conclusion, the probability of error (forgery) lies between L^{-kt} and 2^{-t}, depending on L. Even though this is negligible when $t = \Theta(\log n)$, the larger value must be taken into account when considering the efficiency parameters of the scheme. We get the lowest probability (and hence the best efficiency) when L is a prime number [GQ88] which is large (non-constant, polynomial in $\log n$), provided that the input is of the 'proper' form and that $Y \notin Z_n^*$, for proofs of membership, or $Y \neq 0$, for proofs of knowledge [BD89].

The Schnorr scheme. Let p, q be odd primes with $q \mid p-1$, $\alpha \in Z_p$ have order q, $L = 2^l$, and $x = (v\,; \alpha, p, q, L)$, $v \in Z_p^*$, be the input. The prover A proves that it knows an s such that $v = \alpha^{-s} \bmod p$. Again the protocol has four steps. In Step 1, A sends $z = \alpha^r \bmod p$, r random in $[1 : p-1]$, in Step 2, B sends the random query $e \in Z_L$, and in Step 3, A replies with $y = r + se \pmod q$. In Step 4, B checks that $z = \alpha^y v^e \bmod p$ and accepts if equality holds.

For this protocol the probability of error is $1/2$. Indeed let γ be a primitive element of Z_p and $\alpha = \gamma^{p-1/q} \bmod p$, $\beta = \gamma^{p-1/2q} \bmod p$, and $v = \beta^{-s} \bmod p$, s odd. Then $v \neq \alpha^i \bmod p$ for all i (v has even order) and there is no s such that $v = \alpha^{-s} \bmod p$. $\tilde{A}$ is a dishonest prover which is given s on its knowledge tape. As before $\tilde{A}$ guesses the parity of the query and sends either $z = \alpha^r \bmod p$ or $z = \alpha^r v \bmod p$ in Step 1. In Step 3, $\tilde{A}$ sends

$y = r + se/2 \pmod q$ if e is even, and $y = r + s(e-1)/2 \pmod q$ otherwise. Again B will accept when $\tilde{A}$ has guessed the parity correctly. So the probability of error is 1/2.

In [Sch90, Proposition 2.1] it is argued that if the probability of error ε is greater than 2^{-l+2} then $\log_\alpha v$ can be computed in time $O(\varepsilon^{-1})$ with constant, positive probability. For us, when $l > 3$, this is not true since $\varepsilon = 1/2$ and $\log_\alpha v$ does not exist.

To prevent this situation (of 'proving' knowledge of logarithms which do not exist) the verifier must check in the protocol that $v^q \equiv 1 \pmod p$. Then $\log_\alpha v$ always exists. Of course this is only possible when q is 'public'. The example described above also applies to the Brickell-McCurley identification scheme [BrMcC90] as presented at Eurocrypt'90. This scheme has now been adjusted so that the prover first proves to a Key Issuing Authority that $\log_\alpha v$ exists.

Acknowledgement. The author wishes to thank Yvo Desmedt for helpful discussions and Kevin McCurley for a remark about the Schnorr identification scheme.

References

[BrMcC90] E.F. Brickell, and K.S. McCurley. An interactive identification scheme based on discrete logarithms and factoring. Presented at Eurocrypt'90.

[BD89] M. Burmester, and Y. Desmedt. Remarks on the soundness of proofs. *Electronics Letters*, **25**(22), 1989, pp.1509–1511.

[FFS88] U. Feige, A. Fiat, and A. Shamir. Zero knowledge proofs of identity. *Journal of Cryptology*, **1**(2), 1988, pp. 77–94.

[GQ88] L.C Guillou and J.-J. Quisquater. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory. *Proceedings of Eurocrypt'88*, Lecture Notes in Computer Science 330, Springer-Verlag, Berlin, pp. 123–128.

[FS86] A. Fiat, and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. *Proceedings of Crypto'86*, Lecture Notes in Computer Science 206, Springer-Verlag, New York, pp. 186–194.

[GMR89] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *Siam J. Comput.*, **18**(1), 1989, pp. 186–208.

[OO88] K. Ohta, and T. Okamoto. A modification of the Fiat-Shamir scheme. *Proceedings of Crypto'88*, Lecture Notes in Computer Science 403, Springer-Verlag, New York, pp. 232–243.

[Sch90] C.P. Schnorr. Efficient Identifications and Signatures for Smart Cards. *Proceedings of Crypto'89*, Lecture Notes in Computer Science 435, Springer-Verlag, New York, pp. 239–251.