To quantify the effect of E_s on the code's performance in a noisy channel, the symbol error rate (SER) of the decoded stream is plotted against the channel's bit error rate (BER) or crossover probability, p, as shown in Fig. 2. For comparison, the source was also encoded using a Huffman code. The performance of the randomly-assigned Tunstall code is marginally better than that of the Huffman code. This was expected because Tunstall coding does not suffer from loss of synchronisation of the codewords. When the Tunstall code is optimised, its error performance approaches that of the uncompressed stream. Note, however, that Tunstall coding pays a penalty in code rate; while the Huffman algorithm achieves a code rate of 1.526 (a coding efficiency of 97.7%), the Tunstall algorithm has a code rate of 1.302 (an efficiency of 83.3%) when 8 bit codewords are used. It is possible to improve the compression of the Tunstall algorithm by using longer codewords; while this would not adversely affect either the compression or decompression speed, it would considerably increase the memory requirements. Also, any algorithm for minimising E_s would become significantly slower due to the increased search space.

Table 1: Comparison of assignment algorithms

Algorithm	Error span
Random	2.575
Sequential	1.870
Gray code	1.862
Tabu search	1.555
Simulated annealing	1.343

Conclusions: The algorithms which obtain the best E_s for a Tunstall code tend to be very resource intensive. The fast algorithms, while performing significantly better than random assignment, are much less effective at reducing E_s. In practice, the simple algorithms are the only algorithms that can be used in adaptive compression, and in any other case where the source statistics is not fixed. In certain cases, however, an approximation to the actual source statistics is known, and the complexity of the codeword assignment algorithm is of no consequence. This makes it feasible to seek the best error performance possible.

By increasing the costs of insertion and deletion errors, a code can be designed which trades off substitutional error performance for better synchronisation. This may be useful in image compression and similar applications, where insertion and deletion are typically more visible than substitution errors.

Techniques for further improving the error performance of Tunstall codes, by combining an appropriate error correction scheme with the Tunstall code, are actively being pursued.

26 August 1999
Electronics Letters Online No: 19991365
DOI: 10.1049/el:19991365

J.A. Briffa and V. Buttigieg (*Department of Communications and Computer Engineering, University of Malta, Msida MSD 06, Malta*)

E-mail: jabrif@eng.um.edu.mt

References

1 TUNSTALL, B.P.: 'Synthesis of noiseless compression codes'. PhD Thesis, Georgia Institute of Technology, 1968

2 MAXTED, J.C., and ROBINSON, J.P.: 'Error recovery for variable length codes', *IEEE Trans.*, 1985, **IT-31**, (6), pp. 794–801

3 KRUSKAL, J.B.: 'An overview of sequence comparison: Time warps, string edits, and macromolecules', *SIAM Rev.*, 1983, **25**, (2), pp. 201–237

4 EL GAMAL, A.A., HEMACHANDRA, L.A., SHPERLING, I., and WEI, V.K.: 'Using simulated annealing to design good codes', *IEEE Trans.*, 1987, **IT-33**, (1), pp. 116–123

5 BATTITI, R., and TECCHIOLI, G.: 'The reactive tabu search', *ORSA J. Comput.*, 1994, **6**, (2), pp. 126–140

6 BRIFFA, J.A.: 'Investigation of the error performance of Tunstall coding'. B.Eng. Final Year Dissertation, University of Malta, Faculty of Engineering, 1997

Symmetric identity-proving protocol for smart cards

DaeHun Nyang and JooSeok Song

The concept of a signed subgroup generator is introduced and an interactive proof-based identification and signature scheme is proposed. The scheme is symmetric in the sense that the same computational complexity and hardware for both the prover and verifier are required. It also requires a minimal level of computation and communications for secret information.

Introduction: In a computerised communications system, it is necessary to provide an adequate method by which communicators can identify themselves to each other in an unforgeable manner. The zero-knowledge interactive proof [1 – 3] has played an important role in identification schemes. Here we propose the concept of a 'signed subgroup generator' and design a new interactive proof-based identification scheme and digital signature. The scheme is suitable for smart cards as it requires only one secret number and one accreditation to complete the interactive proof. In the proposed protocol setting, the prover and verifier have the same computational complexity and hardware design, which is useful for mutual identification. Our scheme can be easily modified to serve as a key exchange protocol.

Identification scheme using signed subgroup generator: The proposed interactive protocol is a proof of knowledge of a predicate $P(s, x) = [s^x \equiv g \bmod pq]$, where $\gcd(x, \lambda(pq)) = 1$, and g is a generator of a sufficiently large subgroup of Z/nZ (λ is the Carmichael function). In the protocol, a trusted centre signs 'g' with a private key corresponding to the public key which is certified by a trusted centre. Thus, each user keeps 'the signed g' as its secret information, but does not know the private key with which g is signed. As in other identification schemes, the proposed protocol comprises two steps. The first is the smart card issuing step, and the second is the interactive proof. A trusted centre randomly chooses two large primes, p and q. The two primes are kept securely by the trusted centre. We assume that $n = pq$ is a 768 bit or 1024 bit public number, and the factorisation of n is still unfeasible. Another public value g is also chosen by the trusted centre. g is a generator of a sufficiently large subgroup of Z/nZ. It should be selected by the trusted centre to satisfy $g^k \equiv 1 \bmod n$, where k is the order of g mod n. k must not be smooth and must be large enough (160 bits) to be strong against attacks such as the baby-step giant-step and index calculus attacks. The trusted centre publishes $(n = pq, g)$ in the public directory. The modulus n and the subgroup generator g will be shared among a group of users. When an eligible user applies for a smart card, the trusted centre issues a string I which contains information about the user and the card. The trusted centre then performs the following steps to compute the secret information s_i and a public key v_i for user i.

(i) For a user i who requests the secret value of a trusted centre, the trusted centre chooses v_i, where v_i is prime and $\gcd(v_i, \lambda(n)) = 1$.

(ii) The centre computes $s_i \equiv g^{1/v_i} \bmod n$. s_i can be easily obtained by computing $g^{d_i} \bmod n$ where $v_i d_i \equiv 1 \bmod \phi(n)$.

(iii) The centre generates a signature $S = \text{signature}(I, v_i)$, and the certificate $C(\text{user } i) = (I, v_i, S)$.

(iv) A smart card containing the user's certificate is issued.

Here, the certificate can be generated by a trusted centre using any well-known signature schemes or the proposed signature scheme. A Rabin-like digital signature scheme or low encryption exponent RSA can be used for a faster certificate verification [4]. They require only a few multiplications in the verification step. After the preparatory steps, the prover has a secret number s_i and can prove its identity to the verifier as follows:

(i) The prover sends its certificate $C(\text{prover})$ to the verifier.

(ii) The verifier checks the prover's certificate $C(\text{prover}) = (I, v_i, S)$.

(iii) The prover picks a random number $r \in \{2, ..., n - 1\}$ and sends $x \equiv r^{v_i} \bmod n$ as a test to the verifier.

(iv) The verifier sends a random number $e \in \{1, ..., 2^t\}$ as a question to the prover, where $2^t < v_i$. The size of 2^t represents a compromise between speed and security.

(v) The prover sends to the verifier as a witness: $y \equiv r s_i^e \bmod n$.

(vi) The verifier checks that $x \equiv y^{v_i} g^{-e} \bmod n$ and accepts the proof as valid only when the above result is correct.

The above interactive proof requires only one security number and one accreditation for the proof of identity, but still provides a security level of 2^{-t}. To reduce the number of bits communicated, the prover sends only the first t bits of a hash function $h(x)$ to the verifier in step (iii), and compares $h(x)$ with the first t bits of $y^{v_i}g^{-e}$ mod n. Thus, the total number of communication bits is $2t + \log n$. The protocol requires an inverse operation to compute g^{-e} mod n, but the computation is already in the preprocessing stage. Even though an attacker records a polynomial number of proofs, she cannot increase the probability of cheating, i.e. the protocol is history-independent on a polynomial number of proofs of identity. Using an interactive proof-based identification scheme and a hash function, a secure digital signature scheme under the random oracle model can be constructed [1]. Changing the identification scheme to a signature scheme, we replace the verifier's role by the hash function h.

Completeness and soundness proofs: For the validity and security of the proposed interactive proof, the completeness and soundness of the protocol should be considered. In this Section, we give formal proofs of the protocol.

Theorem 1 (Completeness): If the prover and verifier follow the protocol, the verifier always accepts the prover's proof of identity.

Proof of theorem 1: By definition $y^{v_i}g^{-e} \equiv (rs_i^e)^{v_i}g^{-e} \equiv r^{v_i}(s_i^{v_i})^e g^{-e} \equiv r^{v_i}g^e g^{-e} \equiv r^{v_i} \equiv x \bmod n$. □

The soundness proof that the cheating probability of a dishonest prover cannot be increased to $> 2^{-t}$ is similar to that in [2].

Theorem 2 (Soundness): We assume that the prover does not know the s_i and cannot compute in polynomial time the v_ith root. If the verifier follows the protocol, she will accept the proof as valid with probability bounded by 2^{-t}.

Proof of theorem 2: To increase the probability of cheating, the prover must choose x in such a way that she can compute the v_ith roots y' and y'' of xg^e mod n for the two questions e' and e''. However, the following procedure reveals s_i and contradicts the assumption that the v_ith root cannot be computed in polynomial time without knowing s_i:

(i) For two questions e' and e'', choose Bezout coefficients m and k such that $v_i m + (e' - e'')k = \pm 1$. The Bezout coefficients m and k always exist, because $\gcd(v_i, e' - e'') = 1$.

(ii) Compute the following and output:

$$\left(g^m\left(\frac{y'}{y''}\right)^k\right)^{\pm 1} \equiv \left(s_i^{v_i m}\left(\frac{y'}{y''}\right)^k\right)^{\pm 1} \equiv \left(s_i^{v_i m} g_i^{(e'-e'')k}\right)^{\pm 1} \equiv s_i \bmod n \quad \square$$

If the question e is predicted by the prover, she can deceive the verifier by guessing e such that v_i divides $r + e$ and sending $x \equiv g^r$ mod n and $y \equiv g^{(r+e)/v_i}$ mod n. The verifier will accept the proof of knowledge, because

$$y^{v_i}g^{-e} \equiv \left(g^{(r+e)/v_i}\right)^{v_i} \equiv g^{r+e}g^{-e} \equiv x \bmod n$$

However, the probability of this event is 2^{-t}, and for a sufficiently large t, it is almost impossible to guess a question e. There is a tradeoff between speed and security. If a security parameter t is large, the speed drops. In the protocol, ($x \equiv r^{v_i}$ mod n) is a random number, and y is masked by a random number r which cannot be computed by a verifier who does not know the factorisation. Thus, all the messages from the prover to the verifier do not reveal any information about the prover's secret, s_i.

Why is v_i a prime number?: We will show that the probability of cheating may be $> 2^{-t}$, unless v_i is a prime. For this, we assume that v_i is not a prime. Suppose there is a dishonest prover i, who has (s_i, v_i) such that $s_i^{v_i} \equiv g$ mod n pretends to be prover j. If $\gcd(v_i, v_j) \neq 1$ such as $v_i = la$, $v_j = lb$ and $b < 2^t$, then she can pretend to be prover j with a probability $b^{-1} > 2^{-t}$ by guessing e such that b divides $e + r$, and sending $x \equiv g^r$ mod n and $y \equiv s_i^{(e+r)a/b}$ mod n. Indeed

$$y^{v_j}g^{-e} \equiv s_i^{(e+r)v_i a/b}g^{-e} \equiv s_i^{(e+r)lba/b}g^{-e} \equiv s_i^{v_i(e+r)}g^{-e} \equiv g^r \equiv x \bmod n$$

Thus, a dishonest prover i can cheat a verifier with a probability greater than 2^{-t}. However, if v_i is a prime, this cannot happen.

Consideration of common modulus: The protocol in this Letter uses the same security assumption as that of the RSA scheme. That is, finding the vth root in Z/nZ is as difficult as the factorisation. Simmons has shown that the protocol using common a modulus in the RSA scheme fails as a privacy channel if a message is encrypted and sent to two or more receivers [5]. In that case, an outsider (not a subscriber/user) using only the public key could decrypt the ciphertext with an unacceptably high probability. Also, De Laurentis has shown that the common modulus protocol is even more vulnerable to attack by insiders (subscriber/user) who can break the cryptosystem by using either a probabilistic or a deterministic method [6]. Knowledge of a single encryption/decryption pair is equivalent to factoring the modulus n probabilistically, and enables a subscriber to find other users' secret keys deterministically. Thus, a protocol using the RSA scheme should not use a common modulus. There are two security aspects to be considered in the proposed scheme. One is whether a subscriber (a legal prover) can find d_i from $g^{1/v_i} \equiv g^{d_i}$ mod n and v_i. If she finds d_i, she can easily factor n by [6]. To determine d_i only from g^{d_i} mod n, she should solve a discrete logarithm problem. In fact, most sub-exponential algorithms for solving the discrete logarithm problem assume a finite field F_p or a Galois field $GF(p^m)$. The order of g mod p or g mod p^m is known *a priori* in these fields, whereas the order of g mod n is not known. Thus, these algorithms are not applicable to find d_i only from g^{d_i} in Z/nZ. Moreover, it is equivalent to breaking the RSA digital signature scheme to find d_i from g^{d_i} mod n and v_i. The other aspect to be considered is whether a subscriber can compute another subscriber's secret information g^{1/v_j} mod n from its secret g^{1/v_i} mod n, where v_i and v_j are primes. Unless $v_i = av_j$ (a = 1, 2, ...), g^{1/v_j} mod n cannot be computed with g^{1/v_i} without knowledge of the factorisation [7].

Performance evaluation: In the identification protocol and the signature scheme, pre-computations can reduce the verifier's burden as well as the prover's. The prover can pre-compute $x \equiv r^{v_i}$ mod n in its idle time, and the verifier can prepare g^{-e} mod n in advance. When the protocol starts, the only multiplications the prover need perform are s_i^e mod n. Similarly, it is sufficient for the verifier to compute y^{v_i} mod n and check the validity of the proof. This pre-computation involves half of the verifier's computation.

Table 1: Comparison with other identification schemes

Number of multiplications	Prover	Verifier	Communication bytes (x, e, y)
Fiat-Shamir	$18(t(k + 2)/2)$	$18(t(k + 2)/2)$	12 + 3 + 256
Schnorr*	1	$216(1.5l + 0.25t)$	3 + 3 + 17.5
GQ	$36(1.5t)$	$72(3t)$	3 + 3 + 64
Ong-Schnorr*	$35(t(k + 2)/2 - 1)$	$37(t(k + 2)/2 + 1)$	3 + 3 + 64
Proposed scheme*	$36(1.5t)$	$36(1.5t)$	3 + 3 + 64

* requires certificate verification phase

Comparisons with other schemes in terms of the number of multiplications and the amount of required storage are shown in Table 1. Pre-computations are considered. We assume that the identification schemes provide a security level of 2^{-24}. The Rabin-like digital signature scheme and the low encryption exponent RSA adds only a couple of multiplications in the certificate verification step [4]. We assume that the square and multiply algorithm is used to exponentiate a number. In Table 1, t represents the security level and l the number of bits of q in Schnorr's scheme. k is the number of the prover's secrets, which is proportional to the amount of communication. When the proposed scheme is switched to the digital signature scheme (t = 72), it requires only 14% of the number of multiplications required by the RSA scheme during the signature generation process. In the verification phase 50% of the multiplications required for Schnorr's and Guillous and Quisquater's schemes are required.

Conclusion: We have proposed a new interactive proof-based identification scheme and a digital signature. The scheme is very efficient both in terms of verification and proving steps owing to the

pre-computable protocol structure. This makes it much more appropriate for smart cards and provides computational symmetricity. The proposed identification protocol can also be easily extended to a key exchange protocol.

8 September 1999
Electronics Letters Online No: 19991362
DOI: 10.1049/el:19991362

DaeHun Nyang and JooSeok Song (*Dept. of Computer Science, Yonsei University, SeodaemunGu, ShinchonDong 134, Seoul 120-749, Korea*)

References

1 FIAT, A., and SHAMIR, A.: 'How to prove yourself: Practical solutions to identification and signature problems'. Advances in Cryptology: Proc. Crypto 86, Lecture Notes in Computer Science, (Springer-Verlag, 1987), pp. 186–194
2 QUISQUATER, J.J., and GUILLOU, L.S.: 'A paradoxical identity based signature scheme resulting from zero knowledge'. Advances in Cryptology: Proc. EuroCrypt 88, Lecture Notes in Computer Science, (Springer-Verlag, 1988), pp. 77–86
3 SCHNORR, C.P.: 'Efficient identification and signatures for smart cards'. Advances in Cryptology: Proc. Crypto 89, Lecture Notes in Computer Science, (Springer-Verlag, 1989), pp. 239–252
4 NYANG, D.H., and SONG, J.S.: 'Fast digital signature scheme based on the quadratic residue problem', *Electron. Lett.*, 1997, **33**, (3), pp. 205–206
5 SIMMONS, G.J.: 'A weak privacy protocol using the RSA cryptoalgorithm', *Cryptologia*, 1983, **7**, pp. 180–182
6 DELAURENTIS, J.M.: 'A further weakness in the common modulus protocol for the RSA cryptoalgorithm', *Cryptologia*, 1984, **8**, (3), pp. 253–259
7 EVERTSE, J.-H.: 'Which new RSA signatures can be computed from some given RSA signatures?'. Advances in Cryptology: Proc. EuroCrypt 90, Lecture Notes in Computer Science, (Springer-Verlag, 1991), pp. 83–97

74GHz dynamic frequency divider using InAlAs/InGaAs/InP HEMTs

K. Murata and Y. Yamane

A 74GHz dynamic frequency divider integrated circuit (IC) that uses 0.1μm InAlAs/InGaAs/InP HEMTs is reported. A digital dynamic T-type flip-flop circuit was adopted to achieve a wide operating frequency range. The IC covers most of the V-band millimetre-wave frequency range, and is faster than any digital dynamic frequency divider reported to date.

Introduction: High-speed frequency dividers are key components in measurement instruments, optical fibre communication systems, and microwave and millimetre-wave communication systems. Circuit operation in the millimetre-wave frequency range is normally achieved by using analogue-type frequency dividers such as the regenerative frequency divider [1] and the injection-locked push-pull oscillator-type frequency divider [2]. However, the operating bandwidths of these frequency dividers are relatively narrow (several gigahertz). Digital dynamic frequency dividers based on a clocked inverter type T-type flip-flop circuit (T-FF) yield a wide operating range but fail to equal the high operation frequency of analogue type frequency dividers. For example, the highest frequencies of operation offered by digital-type dynamic frequency dividers are 63GHz using InAlAs/InGaAs/InP HEMTs [3] and 55GHz using AlGaAs/InGaAs HEMTs [4]. In this Letter we describe a digital dynamic frequency divider integrated circuit (IC) that uses 0.1μm InAlAs/InGaAs/InP HEMTs. The IC simultaneously realises high-frequency operation (74GHz) comparable to that of the analogue frequency divider [1, 2], and has a wide bandwidth operating region which almost covers the entire V-band millimetre-wave frequency range.

Circuit design: Fig. 1*a* shows the block diagram of the dynamic frequency divider IC. The circuit is based on SCFL (source-coupled FET logic) series-gated circuitry. The IC consists of a dynamic T-FF, an output buffer and an open-drain type output driver. The IC has a single-ended signal input, and differential outputs that can be directly connected to an SCFL interface [5].

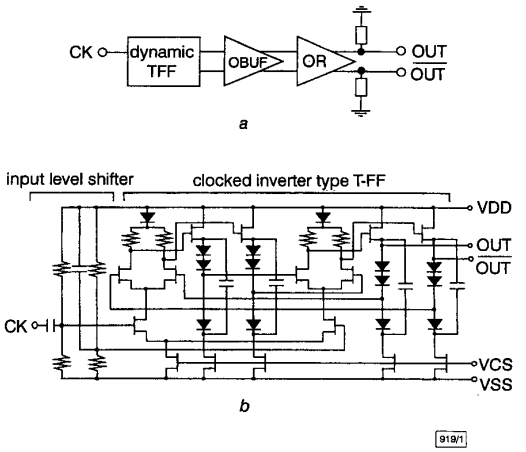

Fig. 1 *Circuit diagrams*
a Frequency divider IC
b Dynamic T-FF

Impedance-matched on-chip 67Ω termination resistors are connected to the output terminals. Fig. 1*b* shows the circuit diagram of the core T-FF. It consists of an input-passive RF level shifter composed of a capacitively coupled resistive divider (the parallel resistance value was set to be impedance-matched 50Ω), and a clocked inverter type dynamic T-FF [6]. The dynamic T-FF has two-level series-gated circuitry, and consists of cascaded two-stage differential inverters, the operating currents of which are controlled by the input clock signal. The operating speed of the T-FF is determined by the gate delay time of the upper-level differential amplifiers, which include the source follower stages [4, 6]. The following three points are taken into account in the present circuit design to shorten the delay time. (i) The input level of the FET of the upper-level differential amplifiers is set to a deeply inverse bias-level in order to reduce the gate-drain capacitance. (ii) The circuit operating bias point of the upper-level differential amplifiers is optimised so as to achieve the highest f_T value by adjusting the FET gate width. The gate width of the upper-level differential amplifiers is 20% smaller than that of the lower-level devices. (iii) The value of the load resistances is optimised so as to minimise the propagation delay time while maintaining the operating frequency range in the V-band. The supply voltage is –5.2V. The chip size of the IC is 2mm × 2mm.

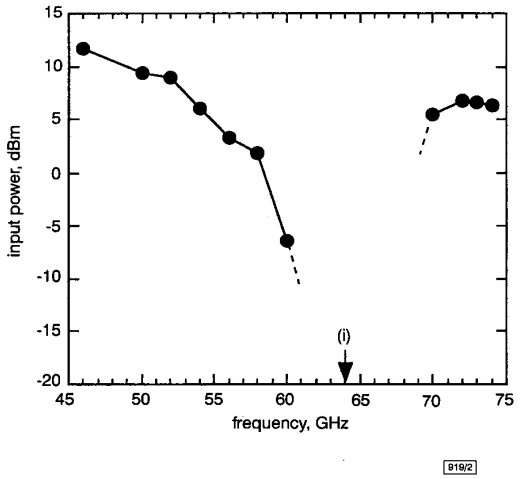

Fig. 2 *Measured sensitivity characteristic*
(i) self-oscillation frequency

Fabrication and experimental results: The IC was fabricated using 0.1μm InAlAs/InGaAs/InP HEMTs [7, 8]. The average threshold