rate, computation costs, and communication costs. Lee and Chang [2] modified the HMP scheme with the same merits but without the use of a one way function. However, neither of them has the public verifiability.

Public verifiability: It is computationally feasible for a judge (who may be the arbiter of the system) to verify the sender's signature without divulging the receiver's private key and the message.

It is necessary for an authenticated encryption scheme to have public verifiability to implement the non-repudiation. Zheng [3] introduced a new type of authenticated encryption termed 'signcryption' which simultaneously satisfies unforgeability, confidentiality, and non-repudiation: but its non-repudiation protocol is inefficient as it is based on the zero-knowledge proof protocol, especially when the non-repudiation procedure is always executed.

In this Letter, we propose an authenticated encryption scheme with public verifiability. Our scheme is as efficient as the signcryption in [3] with respect to both computational costs and the communication overhead. In addition, our scheme has an efficient non-repudiation procedure without using the zero-knowledge proof protocol.

Proposed scheme: Initially, two large primes p and q with $q|(p-1)$ and an element $g \in Z_p^*$ of order q are computed by a trusted third party (TTP for short) and are authenticated to each user. Each user $i \in \{A, B\}$ chooses a secret key $x_i \in Z_q^*$ and computes his public key $y_i \equiv g^{x_i} \bmod p$. He publishes y_i which is certified by the TTP and keeps x_i secret. In addition, the TTP chooses a public one way hash function H with $|H| < |p|$, where $|x|$ denotes the number of bits in x and $|H|$ denotes the number of bits in the output value of hash function H. To send message $m \in Z_p^*$, Alice does the following:

(A-1) picks a random number $k \in Z_q^*$
(A-2) computes $v \equiv (g \cdot y_B)^k \bmod p$ and $e \equiv v \bmod q$
(A-3) computes $c \equiv m \cdot (H(v))^{-1} \bmod p$
(A-4) computes $r = H(e, H(m))$
(A-5) computes $s = k - x_A \cdot r \bmod q$

Alice then sends (c, r, s) to Bob. After receiving (c, r, s), Bob does the following:

(B-1) computes $v \equiv (g \cdot y_B)^s \cdot y_A^{r(x_B+1)} \bmod p$ and $e \equiv v \bmod q$
(B-2) recovers the message $m \equiv c \cdot H(v) \bmod p$
(B-3) verifies $r = H(e, H(m))$

For public verification, Bob computes

$$K_1 \equiv (y_B^k \bmod p) \bmod q \equiv (y_B^s \cdot y_A^{r x_B} \bmod p) \bmod q$$

and forwards $(H(m), K_1, r, s)$ to an arbitrary TTP. To verify that Alice is the originator of the encryption and signature, the TTP does the following:

(TTP-1) computes $e \equiv (g^s \cdot y_A^r \cdot K_1 \bmod p) \bmod q$
(TTP-2) verifies $r = H(e, H(m))$

Our scheme is best used for small message transmission, but it can be adapted for the case of a long message as follows. Alice partitions message m into $(|p|-1)$-bit blocks $m_1, \ldots, m_t$ (use padding if necessary), and she computes the ciphertext blocks $c_1, \ldots, c_t$ by $c_i = (m_i \oplus c_{i-1}^l) \cdot (H(v))^{-1} \bmod p$ (where c_i^l denotes the most left $(|p|-1)$ bits of c_i and $c_0 = v$) and r, s by (A-4) and (A-5), respectively. Alice than sends $(c_1, \ldots, c_t, r, s)$ to Bob. The rest of the scheme can be modified correspondingly.

Security considerations: Basically, a secure authenticated encryption scheme should satisfy the following properties: unforgeability, confidentiality, and non-repudiation. We now analyse the security properties of our scheme.

Unforgeability: Regarding forging Alice's signature, a dishonest Bob is in the best position to do so, as he is the only person who knows x_B which is required to directly decrypt and verify Alice's encryption and signature, i.e. the dishonest Bob is the most powerful attacker we should look at. Given (c, r, s) generated by Alice, Bob can use his private key to decrypt c and obtain m. Thus the original problem is reduced to one in which Bob is in possession of (m, r, s). The latter is equivalent to the Schnorr's digital signature which is unforgeable [4]. Therefore we conclude that our scheme is unforgeable against adaptive attacks.

Non-repudiation: Once Bob computes $K_1 \equiv (y_B^k \bmod p) \bmod q$, everyone can verify the signature (r, s) of the message m. Therefore it is computationally feasible for any TTP to settle a dispute between Alice and Bob without divulging Bob's private key and the message m.

Confidentiality: If any intruder tries to decrypt the message m, he must first compute at least one of the secrets P_{AB} (the Deffie-Hellman secret key between Alice and Bob), x_B or k. One can know K_1 and compute e, but it is infeasible to compute P_{AB} or v, as discussed in [2]. By known-plaintext attack, one can compute $H(v)$, but it is still infeasible to compute P_{AB}. Therefore our scheme can withstand the known plaintext-ciphertext attack.

Efficiency: To compute an authenticated encryption requires only one exponentiation modulo p, one inversion modulo p, and three hash-function evaluations. Signature generation does not require the computation of inversion modulo q. The cost of decryption and verification includes two exponentiations modulo p, and three hash-function evaluations. For public verifiability, two exponentiations modulo p is needed for Bob and the TTP, respectively. Moreover the TTP needs one hash-function evaluation.

The communication overhead between the sender and receiver is very small, only $|H| + |q|$ bits, the communication cost for public verification being $2(|H| + |q|)$ bits.

Conclusion: We have proposed an efficient authenticated encryption scheme with public verifiability. It has only one exponentiation modulo p for encryption and signature, and two exponentiations modulo p for decryption and verification. In addition, the communication overhead is very small, only $|H| + |q|$ bits, and the non-repudiation procedure is very efficient.

Acknowledgment: This work was partially supported by NSFC under grants 60273049 and 90104005.

9 December 2002
Electronics Letters Online No: 20030190
DOI: 10.1049/el:20030190

Changshe Ma and Kefei Chen (*Department of Computer Science and Engineering, Shanghai Jiaotong University, 1954 Hua Shan Road, Shanghai 200080, People's Republic of China*)

E-mail: mcs@sjtu.edu.cn

References

1 HORSTER, P., MICHELS, M., and PETERSEN, H.: 'Authenticated encryption scheme with low communication costs', *Electron. Lett.*, 1994, **30**, (15), pp. 1212–1213
2 LEE, W.-B., and CHANG, C.-C.: 'Authenticated encryption scheme without using a one way function', *Electron. Lett.*, 1995, **31**, (19), pp. 1656–1657
3 ZHENG, Y.: 'Signcryption and its application in efficient public key solution' ISW'97, *in Lect. Notes Comput. Sci.*, 1998, **1397**, pp. 291–312
4 Pointcheval, D., and Stern, J.: 'Security proofs for signature scheme'. Eurocrypt'96, in *Lect. Notes Comput. Sci.*, 1996, **1070**, pp.387–398.

Precision current and charge amplifiers for driving highly capacitive piezoelectric loads

A.J. Fleming and S.O.R. Moheimani

Piezoelectric transducers are known to be highly capacitive loads that exhibit less hysterisis when driven with current or charge rather than voltage. Compliance feedback current and charge amplifiers are introduced. A secondary output voltage feedback loop is employed to prevent DC charging of capacitive loads and to compensate for any voltage or current offsets in the driver circuit. Low frequency bandwidths in the milliHertz range can be achieved.

Introduction: Piezoelectric transducers have found countless applications in such fields as vibration control, nano-positioning, acoustics and sonar. The piezoelectric effect [1] is a phenomena exhibited by

certain materials where an applied electric field produces a corresponding strain and vice versa. One common theme across the diverse piezoelectric applications literature is the problem of hysteresis in the transfer function between the applied voltage and resulting strain [1]. As discussed in [2] and references therein, a great number of techniques have been developed with the intention of reducing hysteresis. Almost all contributions in this area make reference to the well known advantages of driving piezoelectric transducers with current or charge rather than voltage [3]. Simply by regulating the current or charge, a five-fold reduction in the hysteresis is typical [4]. Unfortunately, owing to practical electronic difficulties, this technique has not been widely accepted as a viable solution. The uncontrolled nature of the output voltage in conjunction with typical circuit offsets, generally results in the load capacitor being charged up. When the output or compliance voltage reaches a power supply rail, the output becomes saturated and distorts. The DC load impedance is normally reduced by the connection of an additional parallel resistor. This method results in poor low frequency tracking and precludes the use of such amplifiers in applications requiring precision scanning.

This Letter introduces a new type of current and charge amplifier capable of providing high accuracy, zero DC offset, ultra-low frequency regulation of current or charge. The compliance feedback current and charge amplifiers contain an additional output voltage feedback loop (resulting in only a single additional opamp) to effectively estimate and reject all sources of DC offset. No tuning is required to nullify the DC amplifier offsets.

Design: Consider the simplified schematic diagram of a compliance feedback current or charge amplifier shown in Fig. 1. Neglecting the compliance controller $C(s)$, the high gain feedback loop works to equate the applied reference voltage v_{ref}, to the sensing voltage v_s. In the Laplace domain, at frequencies well within the bandwidth of the control loop, the load current $I_L(s)$ is equal to $V_{ref}(s)/Z_s(s)$. If $Z_s(s)$ is a resistor R_s, $I_L(s)=V_{ref}(s)/R_s$, i.e. we have a current amplifier with gain $1/R_s$ A/V. If $Z_s(s)$ is a capacitor C_s, $q_L=V_{ref}(s)C_s$, i.e. we have a charge amplifier with gain C_s Coulomb/V.

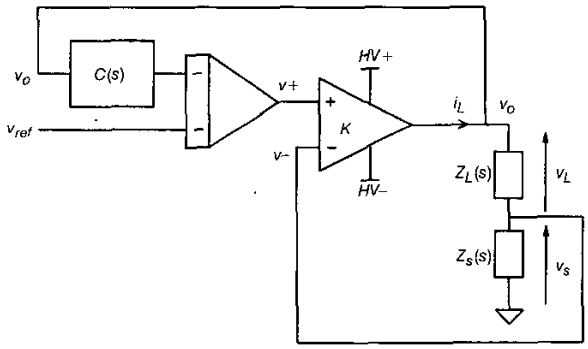


Fig. 1 *Simplified schematic diagram of charge or current amplifier with compliance feedback*

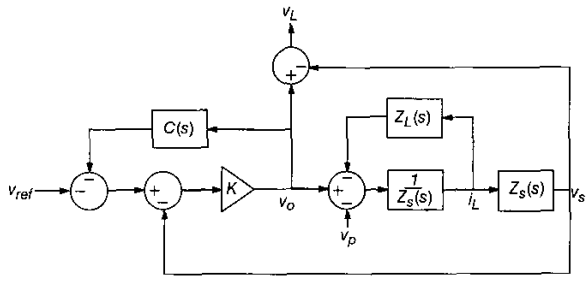


Fig. 2 *Block diagram relating node voltages and currents of loaded amplifier*

The voltages and currents of interest are related in the system block diagram shown in Fig. 2. The auxiliary signal v_p models a load internal voltage source. For example, the piezoelectric voltage internal to a piezoelectric transducer. By definition, the polarity of the source hinders the current i_L.

To control the amplifier, there are two objectives. The first is to ensure good reference current or charge tracking performance. The second is to provide low frequency and DC regulation of the compliance voltage v_o. To understand the trade-off between tracking performance and compliance regulation, the transfer functions of interest are: the transfer function from an applied reference voltage $V_{ref}(s)$ to the voltage measured across the sensing impedance $V_s(s)$, and the transfer function from an applied reference voltage $V_{ref}(s)$ to the compliance voltage $V_o(s)$.

For a current source connected to a capacitive load, i.e. $Z_s(s)=R_s$ and $Z_L(s)=1/C_Ls$, assuming $V_p(s)=0$

$$\frac{V_s(s)}{V_{ref}(s)}=\frac{-KR_sC_Ls}{(1+KC(s))(R_sC_Ls+1)+KR_sC_Ls} \quad (1)$$

$$\frac{V_o(s)}{V_{ref}(s)}=\frac{-KR_sC_Ls-K}{(1+KC(s))(R_sC_Ls+1)+KR_sC_Ls} \quad (2)$$

Proportional-integral (PI) control, $C(s)=(\alpha s+\delta)/s$, achieves complete rejection of DC offset currents while exhibiting a fast settling time in the transient compliance response. Using the variables α, δ and R_s, an arbitrary low frequency bandwidth can be obtained with full control over the system damping. A PI controller is easily implemented with a simple opamp circuit.

For a charge amplifier connected to a capacitive load, i.e. $Z_s(s)=1/C_ss$ and $Z_L(s)=1/C_Ls$,

$$\frac{V_s(s)}{V_{ref}(s)}=\frac{-KC_L}{(1+KC(s))(C_L+C_s)+KC_L} \quad (3)$$

$$\frac{V_o(s)}{V_{ref}(s)}=\frac{-KC_L-KC_s}{(1+KC(s))(C_L+C_s)+KC_L} \quad (4)$$

The compliance controller design for a charge amplifier is considerably easier. Simple integral control ($C(s)=\alpha/s$) results in a first order response with complete regulation of DC offsets.

$$\frac{V_o(s)}{V_{ref}(s)}=\frac{-KC_Ls-KC_ss}{(KC_L+C_L+C_s)s+K\alpha(C_L+C_s)} \quad (5)$$

The location of the closed loop pole is easily manipulated by the variable α.

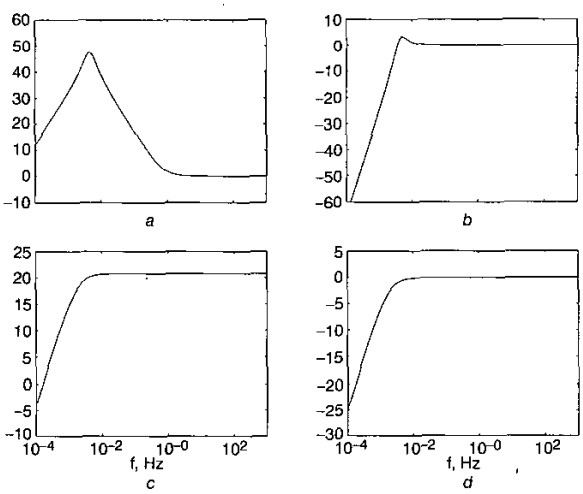


Fig. 3 *Simulated dynamic characteristics of experimental current and charge amplifiers*

a Compliance (current amplifier)
b Tracking frequency (current amplifier)
c Compliance (charge amplifier)
d Tracking frequency (charge amplifier)

Experiments: To illustrate the operation of the current amplifier, a 1 μF capacitor is driven at low frequencies with a current sensing resistor of 220 kΩ. With $C(s)=(0.004s+0.00016)/s$, the simulated compliance and tracking frequency responses, $V_o(s)/V_{ref}(s)$ and $V_s(s)/V_{ref}(s)$ respectively, are shown in Fig. 3*a* and *b*. A 100 mHz signal is applied to examine the low frequency tracking performance. The reference and measured currents are shown in Fig. 4*a*.

Similar experiments were carried out for a charge amplifier. Using a sensor capacitance of 10 μF, the compliance controller $C(s) = 0.001/s$ provides the desired response. Analogous frequency and time domain results are presented in Fig. 3*c* and *d*, and Fig. 4*b*.

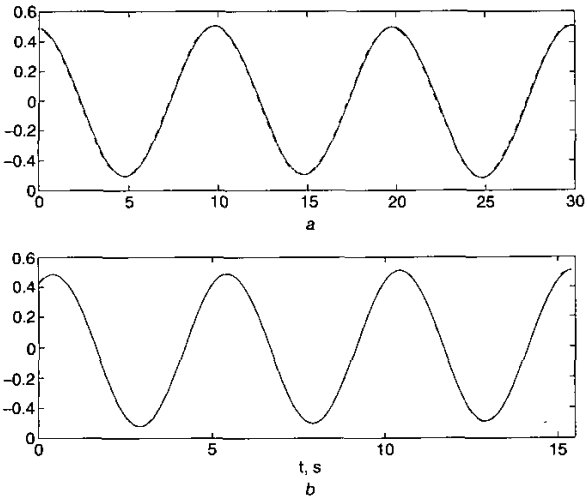


Fig. 4 *Time domain performance of experimental current and charge amplifiers*

a Current amplifier
b Charge amplifier
— reference current
– – measured current

Conclusions: A new type of current and charge amplifier has been introduced. By feeding back the compliance voltage of the amplifier, the effect of DC circuit offsets can be eliminated. Experimental results show excellent low frequency current and charge tracking performance with complete rejection of DC offsets.

16 October 2002
Electronics Letters Online No: 20030235
DOI: 10.1049/el:20030235

A.J. Fleming and S.O.R. Moheimani (*School of Electrical Engineering and Computer Science, The University of Newcastle, University Drive, Callaghan NSW 2304, Australia*)

E-mail: andrew@ee.newcastle.edu.au

References

1 ADRIAENS, H.J.M.T.A., KONING, W.L.D., and BANNING, R.: 'Modeling piezoelectric actuators', *IEEE/ASME Trans. Mechatronics*, 2000, **5**, pp. 331–341
2 FURUTANI, K., URUSHIBATA, M., and MOHRI, N.: 'Improvement of control method for piezoelectric actuator by combining charge feedback with inverse transfer function compensation'. Proc. IEEE International Conference on Robotics Automation, Leuven, Belgium, May 1998, pp. 1504–1509
3 NEWCOMB, C.V., and FLINN, I.: 'Improving the linearity of piezoelectric ceramic actuators', *Electron. Lett.*, 1982, **18**, pp. 442–443
4 GE, P., and JOUANEH, M.: 'Tracking control of a piezoelectric actuator', *IEEE Trans. Control Syst. Technol.*, 1996, **4**, pp. 209–216

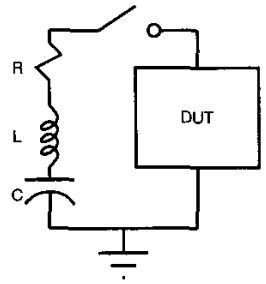
Cancellation technique to provide ESD protection for multi-GHz RF inputs

S. Hyvonen, S. Joshi and E. Rosenbaum

A technique to provide ESD protection for multi-GHz RF inputs is presented. It provides protection against both human body model (HBM) and charged device model (CDM) type events with minimal effect on RF performance. A 5.25 GHz LNA protected by this means has a measured HBM ESD protection level of 3.6 kV.

Introduction: Electrostatic discharge (ESD) is responsible for approximately half of all integrated circuit failures as well as yield loss during manufacturing [1]. Human body model (HBM) events are well-known, but changed device model (CDM) events are becoming dominant with increased semiconductor manufacturing automation [2]. Placing on-chip ESD protection circuits at RF input pins introduces parasitic shunt capacitance that adversely affects the RF circuit performance. Traditionally, minimising this capacitance has been a goal of ESD protection circuit design for RF ICs. However, this approach is not feasible for circuits operating at frequencies higher than 2 GHz [3].

An LCR circuit, as shown in Fig. 1, can model both HBM and CDM type discharges. The component values are taken from [4]. In both cases, the capacitor is precharged to the ESD voltage and then the switch is closed, causing the capacitor to discharge through the device under test (DUT). An HBM event has a relatively long time constant, and its frequency spectrum rolls off in the low MHz range. In contrast, a CDM event model contains an LC resonator with a resonant frequency $f_0 \cong 500$ MHz, giving it an oscillatory response, and the frequency spectrum is significantly affected by the reactive input impedance of the DUT. This poses problems for tuned, narrowband RF circuits.



	HBM	CDM
R	1500Ω	10Ω
L	–	10 nH
C	100 pF	5 pF

Fig. 1 *Models for HBM and CDM events*

Because traditional ESD protection devices add parasitic capacitance, Leroux and Steyaert [5] proposed use of an inductor for ESD protection, as shown in Fig. 2*a*. The inductor, L_{esd}, is chosen to tune out the input parasitic capacitance (C_p) such as the bond pad capacitance, at the RF operation frequency. During a slow HBM ESD event, the inductor acts as a low impedance conduction path, potentially providing very good protection levels. However, the spectrum of a CDM event extends well into the RF band, near the resonant frequency of the L_{esd}–C_p resonator, and thus the impedance of the ESD conduction path will be large and can even cause unwanted oscillations as the resonator is mostly undamped.

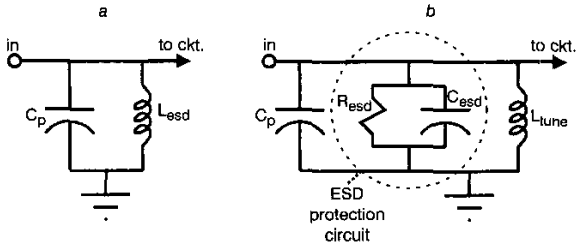


Fig. 2 *L_{esd}–C_p resonator and cancellation protection circuits*

a L_{esd}–C_p resonator
b Cancellation protection circuits
In *b*, R_{esd} and C_{esd} represent an actual ESD protection device. R_{esd} is very large under normal operation conditions, and just a few ohms when device is triggered on

Proposed solution: We present a 'cancellation circuit', in which an explicit ESD protection circuit is added to the input, and the total parasitic capacitance ($C_p + C_{esd}$) is tuned out, i.e. 'cancelled', with an inductor L_{tune}, as shown in Fig. 2*b*. During normal operation, the ESD protection circuit is in its off-state and can be accurately modelled as a parallel RC network [6]. At the RF operation frequency, the inductor is in resonance with the capacitances, leaving only a large shunt