generates several peaks (shown in Fig. 3), and it is difficult to distinguish which peaks are generated by which images of the input. However, the peak values and their corresponding positions shown in Table 1 indicate only four significant peaks. To obtain the images corresponding to these four peaks, the DRFT-based correlator is applied. To see which image in both the reference and the input generates the first peak, we move Fig. 2 40 pixels in the X-direction and 124 pixels in the Y-direction. The moved image is correlated with the input object by the DRFT-based correlator, resulting in the displayed image shown in Fig. 4a, which is the 'A and B' image in the top righthand corner of Fig. 1. By applying the same procedures to the second, third, and fourth peaks, we obtain two single Bs and one single A, shown in Fig. 4b-d. The conclusion of the DRFT-based correlation between Figs. 1 and 2 is that Fig. 1 contains four patterns; 'A and B', two single Bs, and one single A.

Fig. 4 DRFT-based correlator output corresponding to different peaks

a 1st peak
b 2nd peak
c 3rd peak
d 4th peak

Table 1: Seven larger peak values of Fig. 3

Peak number	Peak value	Co-ordinate (x, y)	Corresponding input object	Matching reference object	Detected input object		
					Position	Area (pixels): 128x(peak value)	DRFT-based correlator output
1	0.7969	(40, 124)	Upper right A, B	A, B	A(73.30) B(82.46)	102	Fig. 4a
2	0.5078	(116, 40)	Lower left B	B	(32.98)	65	Fig. 4b
3	0.5078	(117, 91)	Upper left B	B	(38.18)	65	Fig. 4c
4	0.2891	(116, 18)	Left A	A	(17.50)	37	Fig. 4d
5	0.2578	(8, 8)	Z	B	(55.59)	33	
6	0.2188	(54, 100)	X	B	(97.20)	28	
7	0.2031	(31, 43)	Y	B	(73.94)	26	

Conclusion: The DRFT contains both time and frequency information. Thus, the DRFT-based correlator can not only generate correlation peaks, but also display the corresponding correlated images. With this property, the DRFT-based correlator can be used to recognise multiple different objects.

© IEE 1998

Electronics Letters Online No: 19980738

10 April 1998

Neng-Chung Hu and Kuo-Kan Yu (Electronic Engineering Department, National Taiwan University of Science and Technology, 43, Keelung Road, Sec. 4, Taipei, Taiwan, Republic of China)

References

- HORNER, J.L., and BARTELT, H.O.: 'Two-bit correlation', *Appl. Opt.*, 1985, **24**, (18), pp. 2889-2893

- MAHALANOBIS, A., KUMAR, B.V.K.V., and CASASENT, D.: 'Minimum average correlation energy filters', *Appl. Opt.*, 1987, **26**, (17), pp. 3633-3640
- JAVIDI, B., WANG, J., and TANG, Q.: 'Multiple-object binary joint transform correlation using multiple-level threshold crossing', *Appl. Opt.*, 1991, **30**, (29), pp. 4234-4244
- SANTHANAM, B., and McCLELLAN, J.H.: 'The discrete rotational Fourier transform', *IEEE Trans. Signal Process.*, 1996, **SP-44**, (4), pp. 994-998

Improvement of Saeednia's self-certified key exchange protocols

Tzong-Chen Wu, Yuh-Shihng Chang and Tzouh-Yi Lin

In 1997, two self-certified key exchange protocols were proposed by Saeednia. It is shown that Saeednia's self-certified key exchange protocols are insecure in that an adversary may impersonate any legitimate user in key exchange. An improvement against the impersonation attack is described.

Introduction: Saeednia [1] presented two key exchange protocols based on Girault's self-certified public key system [2]. In Saeednia's key exchange protocols, there exists a trusted third party (TTP) for system setup and user registration; however, the TTP does not know the secret key of any user during user registration. Saeednia's key exchange protocols preserve the merits inherent in both the identity-based system and the self-certified system, and hence allow a considerable reduction in communication complexity. In this Letter, we first show that Saeednia's self-certified key exchange protocols are insecure. An adversary may impersonate any legitimate user in running these protocols. We also present an improvement that can withstand the impersonation attack.

Saeednia's key exchange protocol: In the setup of this system, the TTP chooses an integer n as the product of two large distinct primes p and q of almost the same size, such that $p = 2p' + 1$ and $q = 2q' + 1$, where p' and q' are also primes, a base $g \neq 1$ of order $r = p'q'$, a large integer $u < r$, and a one-way hash function f . The TTP makes g, u, f and n public, keeps r secret and discards p and q afterwards. Next, any user U_i can register with the TTP by performing the following steps:

- U_i randomly chooses a secret key $x_i \in Z_u$, computes the public key $y_i = g^{x_i} \bmod n$ and gives it to the TTP.
- The TTP prepares a string I_i associated with U_i 's personal information (name, address, etc.) and computes U_i 's identity $ID_i = f(I_i)$.
- The TTP computes $w_i = y_i^{ID_i^{-1}} \bmod n$ as a witness and sends $\{I_i, w_i\}$ to U_i .
- U_i verifies the identity and the witness by checking that $y_i = w_i^{f(I_i)} \bmod n$.

Saeednia claimed that forging a valid witness w_i for U_i is equivalent to breaking an instance of the RSA cryptosystem [3]. Suppose that U_i and U_j want to exchange a secret key to be used for secure communication. They can perform the following protocols. These protocols are based on the well-known Diffie-Hellman key distribution system [4]. Note that the secret key exchanged in protocol 1 is invariant, while it is time-variant in protocol 2.

Protocol 1

- U_i sends $\{I_i, w_i\}$ to U_j
- U_j sends $\{I_j, w_j\}$ to U_i
- U_i computes the secret key shared with U_j as $k = w_j^{f(I_j) \cdot x_i} \bmod n$
- U_j computes the secret key shared with U_i as $k = w_i^{f(I_i) \cdot x_j} \bmod n$

Protocol 2

- U_i randomly chooses a secret integer $t_i \in Z_u$, computes $v_i = g^{t_i} \bmod n$ and sends $\{I_i, w_i, v_i\}$ to U_j
- U_j randomly chooses a secret integer $t_j \in Z_u$, computes $v_j = g^{t_j} \bmod n$ and sends $\{I_j, w_j, v_j\}$ to U_i
- U_i computes the secret key shared with U_j as $k = w_j^{f(I_j) \cdot t_i} \cdot v_j^{x_i} \bmod n$
- U_j computes the secret key shared with U_i as $k = w_i^{f(I_i) \cdot t_j} \cdot v_i^{x_j} \bmod n$

Note that the secret key shared between U_i and U_j can be regarded as

$$k = y_j^{x_i} = y_i^{x_j} = g^{x_i \cdot x_j} \pmod{n} \quad (\text{in protocol 1})$$

or

$$k = y_j^{t_i} \cdot v_j^{x_i} = y_i^{t_j} \cdot v_i^{x_j} = g^{(x_i \cdot t_j) + (x_j \cdot t_i)} \pmod{n} \quad (\text{in protocol 2})$$

Attack on Saeednia's key exchange protocols: Consider the case that an adversary pretends to act as U_i and tries to exchange a secret key with U_j such that U_j will indeed share the secret key with U_i . First of all, the adversary randomly chooses an integer $\alpha \in \mathbb{Z}_n$. Then he sets $x'_i = \alpha \cdot f(I_i)$ as a fake secret key for U_i and replaces U_i 's original public key y_i (maintained by the TTP) with $y'_i = g^{x'_i} \pmod{n}$. Thereafter, the adversary can easily compute a valid witness $w'_i = g^\alpha \pmod{n}$ for U_i , since the substituted public key $y'_i = g^{\alpha \cdot f(I_i)} = w'^{\alpha \cdot f(I_i)} \pmod{n}$ is also self-certified. In protocol 1, if the adversary sends $\{I_i, w'_i\}$ to U_j in step (i) and intercepts the message $\{I_j, w_j\}$ that is intended to be sent to U_i in step (ii), both the adversary and U_j will share the same secret key $k' = w'^{f(I_j) \cdot x_j} = w_j^{f(I_i) \cdot x_i} = g^{x_i \cdot x_j} \pmod{n}$. Moreover, U_j will believe that he indeed communicates with U_i , because the pair (y'_i, w'_i) will be authenticated successfully. It can be seen that protocol 2 is also vulnerable to such an attack.

Our improvement: The weakness of Saeednia's key exchange protocols is that the witness w_i computed by the TTP is not self-certified, although to forge a valid w_i is equivalent to breaking an instance of the RSA cryptosystem. We can easily remove this weakness by replacing step (iii) of the user registration phase with

(iii*) The TTP computes $w_i = (y_i - ID_i)^{ID_i^{-1}} \pmod{n}$ as a witness and sends $\{I_i, w_i\}$ to U_i .

Our improvement only requires one more subtraction than the original step. Note that $y_i = g^{x_i} = (w_i^{ID_i} + ID_i) \pmod{n}$. This implies that, without knowing x_i , any adversary can easily compute an authenticated pair (w_i, y_i) for U_i satisfying the check in step (iv) of the user registration phase. However, the adversary still does not know U_i 's secret key x_i unless he can solve the problem of computing discrete logarithm modulo a large composite [5, 6]. Since x_i is unknown, the adversary cannot pretend to act as U_i to share a secret key with U_j . That is, in steps (iii) and (iv) of protocols 1 and 2, the adversary and U_j cannot obtain the same secret key.

© IEE 1998

24 March 1998

Electronics Letters Online No: 19980797

Tzong-Chen Wu, Yuh-Shihng Chang and Tzouh-Yi Lin (Department of Information Management, National Taiwan University of Science and Technology, 43, Section 4, Keelung Road, Taipei, Taiwan 106, Republic of China)

E-mail: tcwu@cs.ntust.edu.tw

References

- 1 SAEEDNIA, S.: 'Identity-based and self-certified key-exchange protocols'. Proc. Information Security and Privacy Second Australasian Conf., Sydney, Australia, 7-9 June 1997, pp. 303-313
- 2 GIRAULT, M.: 'Self-certified public keys'. Advances in Cryptology - Eurocrypt '91, 1991, (Springer-Verlag), pp. 491-497
- 3 RIVEST, R.L., SHAMIR, A., and ADLEMAN, L.: 'A method for obtaining digital signatures and public key cryptosystems', *Commun. ACM*, 1978, **21**, (2), pp. 120-126
- 4 DIFFIE, W., and HELLMAN, M.E.: 'New directions in cryptography', *IEEE Trans. Inf. Theory*, 1976, **IT-22**, (6), pp. 135-145
- 5 BRICKELL, E.F., and MCCURLEY, K.S.: 'An interactive identification scheme based on discrete logarithms and factoring'. Advances in Cryptology - Eurocrypt '90, (Springer-Verlag, 1990), pp. 63-71
- 6 GIRAULT, M.: 'An identity-based identification scheme based on discrete logarithms modulo a composite number'. Advances in Cryptology - Eurocrypt '90, (Springer-Verlag, 1990), pp. 481-486

40Gbit/s EAM driver IC in SiGe bipolar technology

R. Schmid, T.F. Meister, M. Rest and H.-M. Rein

An SiGe bipolar IC for directly driving a differential electroabsorption modulator in a 40Gbit/s fibre optic TDM system is presented. An adjustable modulator bias voltage (0 to -2V) is generated on-chip by a novel active network in the output stage. Clear eye diagrams at 40Gbit/s and output swings up to 2.5V_{pp} (nominal 2V_{pp}) were measured on mounted chips.

Introduction: Today, there is a worldwide trend towards increasing the data rate in fibre optic TDM systems from 10 to 40Gbit/s (c.f. [1]). A severe bottleneck in the electronics of such a system is the modulator driver on the transmitting side. This is because of the contradicting demands on high voltage swing and high operating speed [2]. Electroabsorption modulators (EAM) need a lower voltage swing compared to Mach-Zehnder interferometers (MZI) and may, therefore, be more suitable to be driven by monolithic integrated circuits (rather than by expensive hybrid amplifiers). However, as one disadvantage, the EAM represents a capacitive load, in contrast to the 50Ω input of an MZI. As a consequence, at 40Gbit/s it would be extremely difficult to drive the modulator via a 50Ω transmission line. In this case, due to insufficient matching, double-reflections would occur which increase time jitter. To solve these problems, we preferred (in contrast to the usual practice) to bond the driver outputs directly to the EAM chip. High-speed performance is further improved and mounting costs are reduced by implementing the (low-ohmic) load resistors as well as the EAM biasing on the driver chip.

Promising results at 30Gbit/s have been published for ICs in III-V compound semiconductors which show single-ended voltage swings of 2.2V_{pp} [3, 4], while in the presentation corresponding to [4], even 40Gbit/s at 2.9V_{pp} swing is claimed. However, all these results were achieved for on-chip measurements only. Moreover, capacitive loading by an EAM and the resulting problems, mentioned above, are not considered.

To reliably achieve 40Gbit/s with the SiGe bipolar technology available here, we must reduce the voltage swing at the driver output. For this, a symmetrical EAM configuration was used which can be driven by differential signals with a voltage swing of 2V_{pp} (2 × 1V_{pp}).

Fig. 1 Circuit concept of modulator driver

Alternative loading by differential EAM or sampling scope is indicated

Circuit design: Fig. 1 shows the circuit concept of the driver IC, which consists of two current switches (CS1, CS2) each driven by three emitter follower (EF) pairs, as in our previously published designs [2, 5]. However, due to the direct coupling of driver and EAM chip, the output stage must now be much more sophisticated.

First, the output current switch (CS2) is extended to a cascode configuration by a grounded-base stage (GBS), which mitigates potential breakdown problems of the output transistors and, moreover, slightly increases operating speed. Owing to the strong capacitive loading by the EAM, the output time constant must be reduced by low output resistances (nominal $R_O = 25\Omega$), requiring a high switching current in the output stage (nominal $\Delta I = 40\text{mA}$). For generating the EAM bias, the output resistors are connected to cascaded EFs (EF1, EF2). The bias voltage V_{Bias} equals the