PHILIPS

Finite Field Multipliers for Ultra-Constrained Environments

Jorge Guajardo[1], Sandeep S. Kumar[1],

Tim Kerins[2], and Pim Tuyls[3]

[1]Philips Research, Eindhoven, Netherlands
[2]Dept. Electrical and Electronic Eng., University College Cork, Ireland
[3]Business Unit Intrinsic-ID, Philips Research, Eindhoven, Netherlands

2nd Benelux Workshop on Information and System Security
WISSEC 2007
September 20-21, 2007

Contents

Counterfeiting of Goods

- $400 Billion/Yr
- Revenue losses
  - Pay-TV: $1.5 Billion/Yr
  - Spare Parts: $3 Billion/Yr
  - Electronic Companies (Cisco, HP, Nortel, 3Com): $100 Billion/Yr
- Harms People:
  - Murder by Medicine [Nature]
  - National Security
- Damaged Brand

[Source: Pira International Ltd 2005, IEEE Spectrum, May 2006]

Relevant?

The New York Times
nytimes.com

PRINTER-FRIENDLY FORMAT
SPONSORED BY

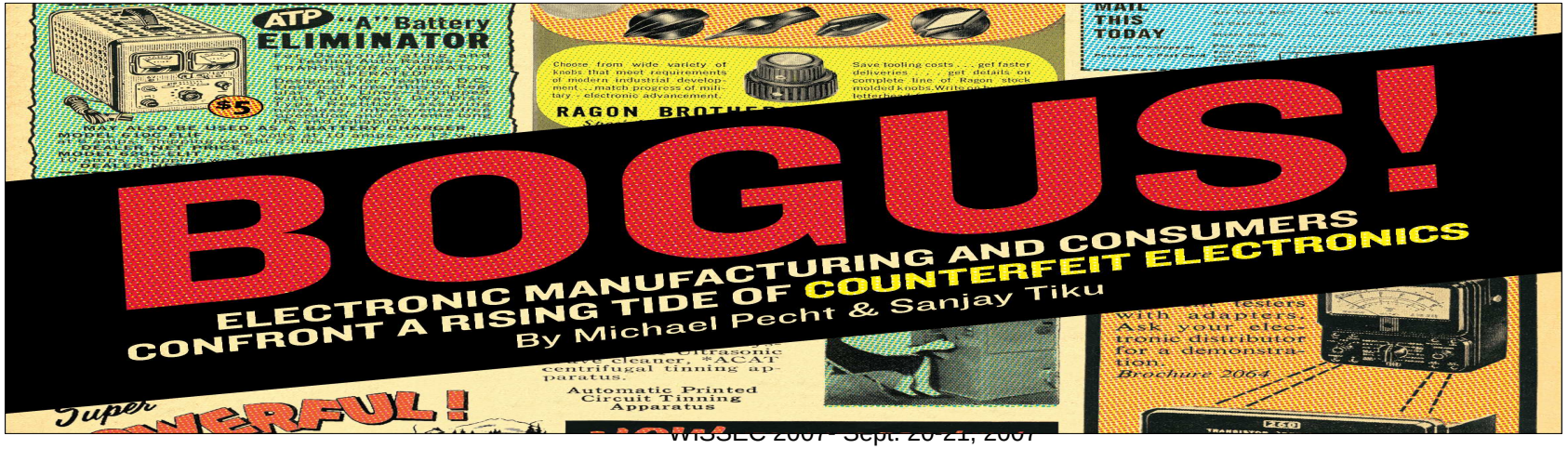
May 1, 2006

Next Step for Counterfeiters: Faking the Whole Company

By DAVID LAGUE

BEIJING — At first it seemed to be nothing more than a routine case of counterfeiting in a country where faking it has become an industry.

In mid-2004, managers at the Tokyo headquarters of the Japanese electronics giant NEC started receiving reports that pirated keyboards and blank CD and DVD discs bearing the company's brand were on sale in retail outlets in Beijing and Hong Kong. So like many other manufacturers combating intellectual property thieves in China, the company hired an investigator to track down the pirates.



Relevant?

The New York Times
nytimes.com

PRINTER-FRIENDLY FORMAT SPONSORED BY

May 1, 2006

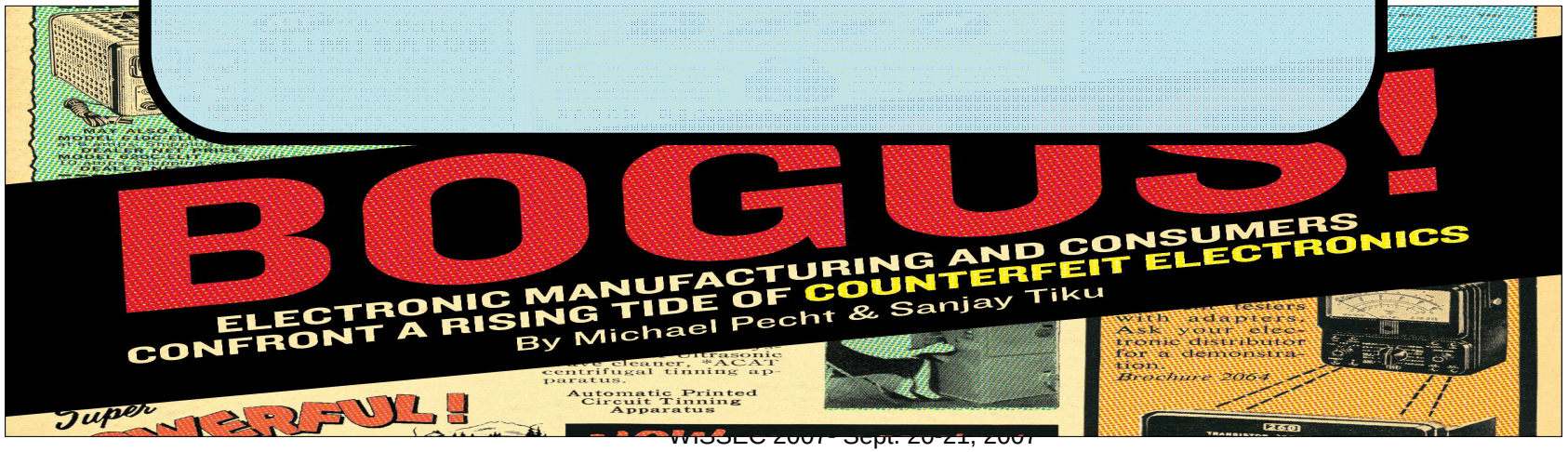
Next Step for Counterfeiters: Faking the Whole Com

By DA

BEIJ ... in a coun

In mi ... EC starte ... the comp ... other manu ... inves

10% of all High Tech Products sold are Counterfeit!



Idea: make RFID-tags suitable for anti-counterfeiting

Embed an RFID-tag into product or package

RFID tag gets secret information on which it can be authenticated

Requirement: Withstand a cloning attack

Produce a new Tag (chip) containing the original secret authentication information

Reader can then not distinguish a cloned from an authentic chip

Contents

Authentication Options - PUFs

- Derive strings from a complex physical system that is inherently uncloneable (e.g. a large number (10^{10}) of randomly distributed particles).

- PUF = Physical Unclonable Function
  - Easy to evaluate (by probing the physical system)
  - Inherently tamper resistant
  - Manufacturer not-reproducible
  - PUFs can be used as a source of a large amount of unclonable secret key material

- Unclonable:
  - Hard to make a physical clone
  - Hard to make a mathematical model that simulates the behaviour of the physical structure

Authentication Options with PUFs

- Online verification
  - Requires to be connected permanently to DB
  - Large number of Challenge-Response Pairs

- Off-line verification (Tuyls and Batina, CT-RSA 2006)
  - **Physical protection**
    - Unforgeable/uncloneable structures embedded in the product (its package)
    - Derive a fingerprint from the structure and print it on the product
  - **Cryptographic Protection**
    - Digital signatures: prevents tampering with the fingerprints and auxiliary data
    - Secure Identification Protocols

Contents

Authentication Options

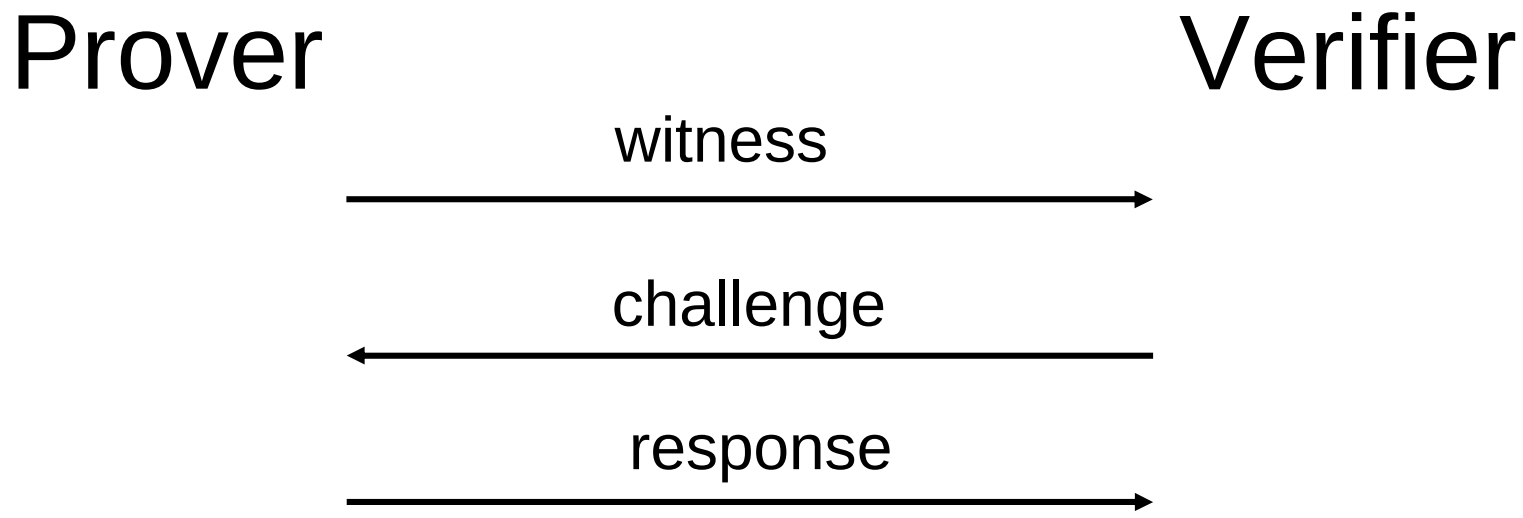
Options:

- ECDSA Signature
  ➡ one point multiplication + hash
- Identification Protocols: Schnorr or Okamoto
  ➡ one or two point multiplications

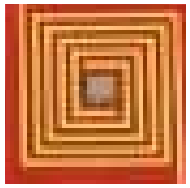
Secure Identification Protocols

Set-up: an elliptic curve $E(GF(2^m))$
a point P of order n and a commitment $Z = aP$ to the secret a

Protocol Anatomy



Schnorr Identification Protocol



Tag
(*a*)

Reader
(Z=aP)

1. request

2. Choose $r \in_R [1, n-1]$

3. Compute $X = rP$

4. X

5. Choose challenge

$2 \le r \le 2^t < n$

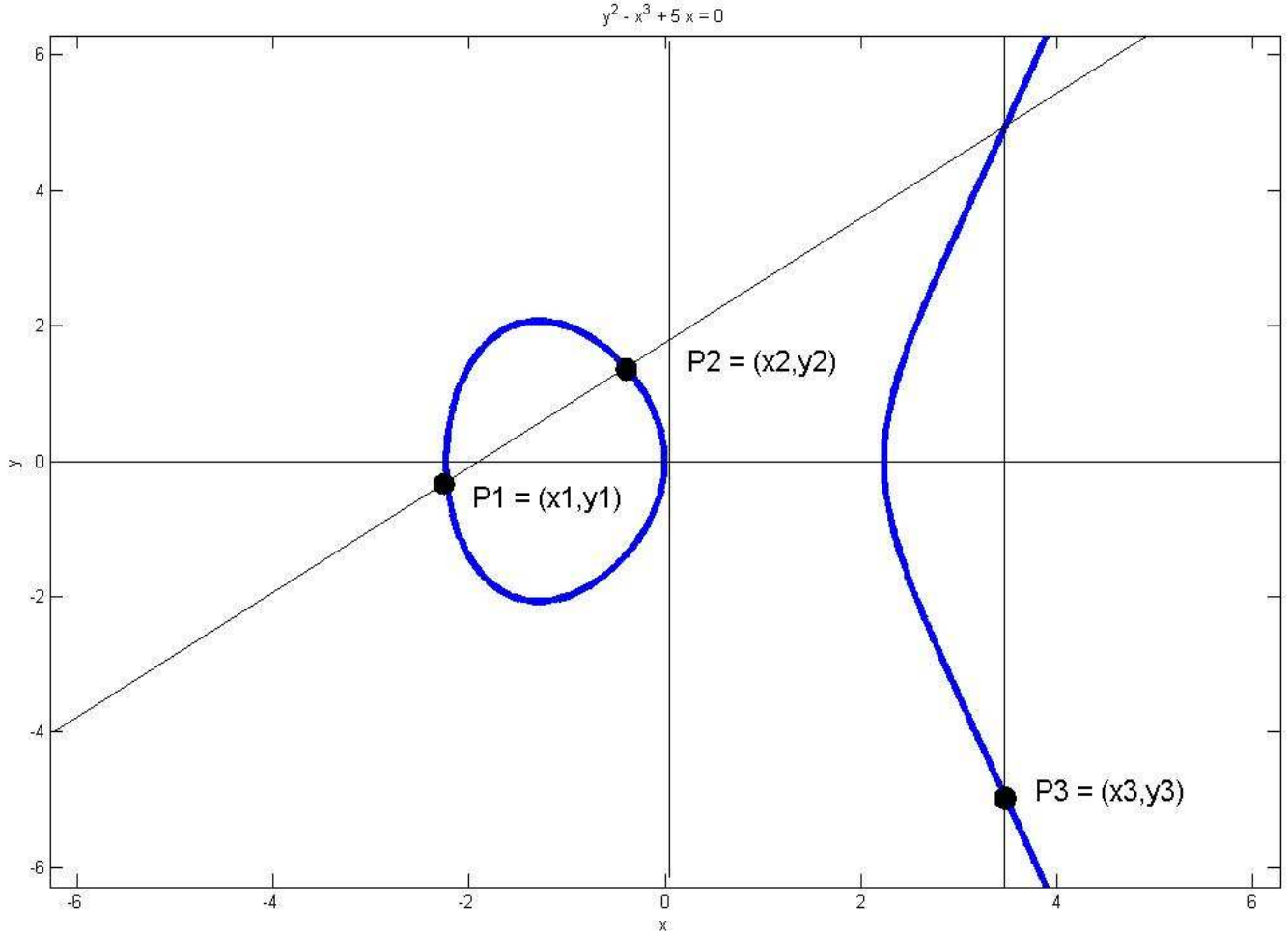
6. c

7. Compute $y = ac + r \bmod n$

7. y

8. If
   $yP - eZ = X = rP$
   $(ac + r)\,P - c(aP) = X$
   accept
   Else
   reject

Elliptic Curve Group Operation



Elliptic Curve Group Operation (continued)

Given an elliptic curve E

$$E : y^2 + xy = x^3 + ax + b$$

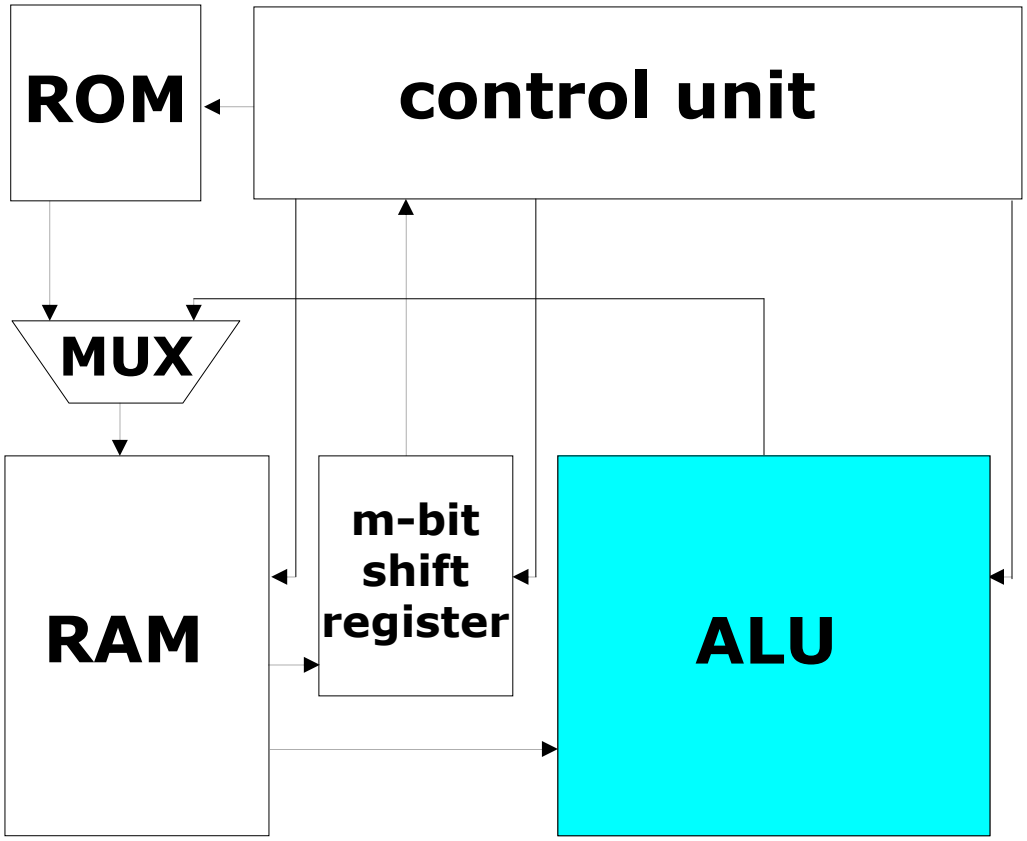
and points $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$, we define

$$P_3 = (x_3, y_3) = P_1 + P_2$$

$$P_3 = \begin{cases} x_3 = \lambda^2 + \lambda + x_1 + x_2 + a, \;\; \lambda = \left(y_1 + y_2\right) \Big/ \left(x_1 + x_2\right) \\ y_3 = \lambda\left(x_1 + x_3\right) + x_3 + y_1 \end{cases}$$

Contents

EC Processor Architecture



How do we multiply in $GF(2^m)$?

Need an irreducible polynomial $q(x)$, then $q(\alpha)=0 \Rightarrow \alpha^m = Q(\alpha)$

Assume polynomial basis representation of elements in $GF(2^m)$

Let

$$A(\alpha), B(\alpha) \in GF(2^m)$$

Then

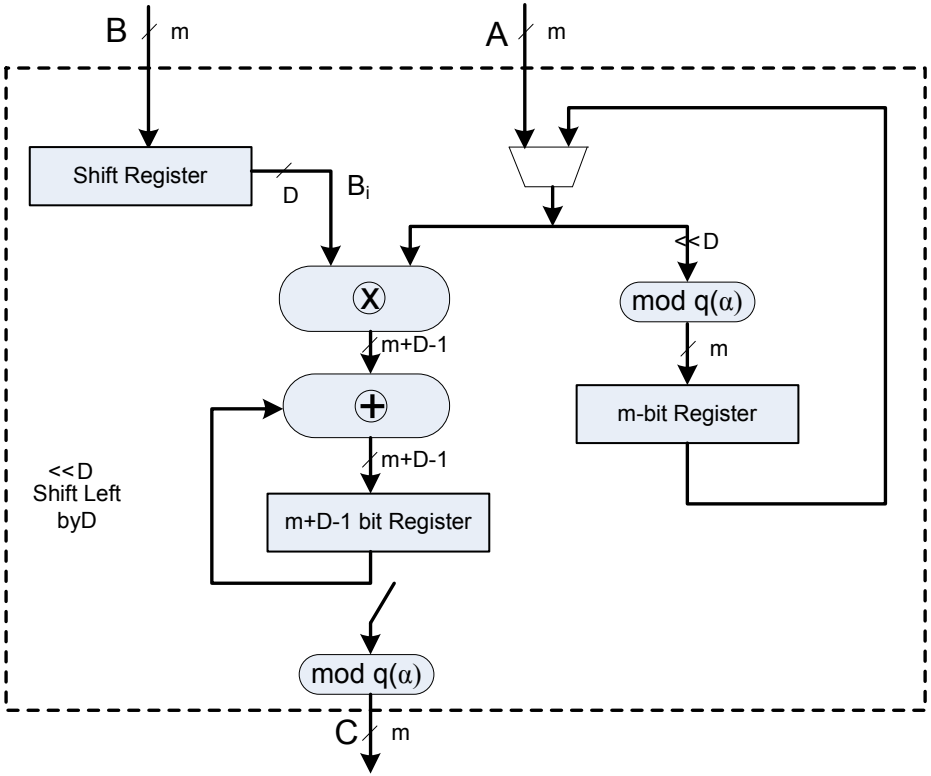
$$C(\alpha) \cong A(\alpha)\cdot B(\alpha) \cong A\sum_{i=0}^{m-1} b_i \alpha^i \mod q(\alpha)$$

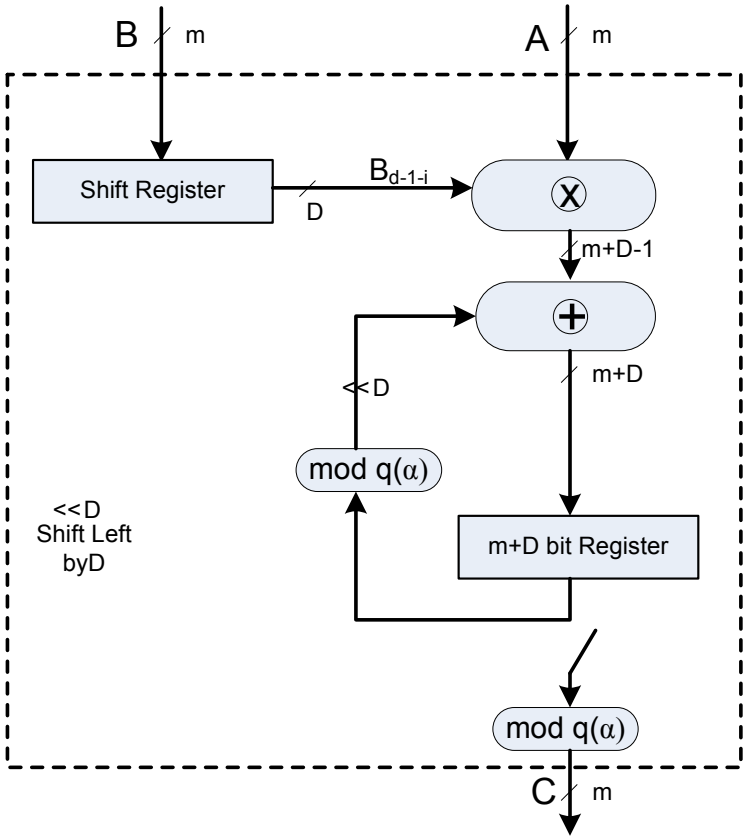
But also

$$C(\alpha) \cong A\sum_{i=0}^{d-1} B_i \alpha^{Di} \mod P(\alpha), \quad B_i = \sum_{j=0}^{D-1} b_{Di+j}\alpha^j, \; d = \text{ceil}\left(\frac{m}{D}\right)$$

What does this look like in hardware?

$$C(\alpha) \cong A\sum_{i=0}^{d-1} B_i \alpha^{Di} \mod q(\alpha), \quad B_i = \sum_{j=0}^{D-1} b_{Di+j}\alpha^j, \; d = \text{ceil}\left(\frac{m}{D}\right)$$

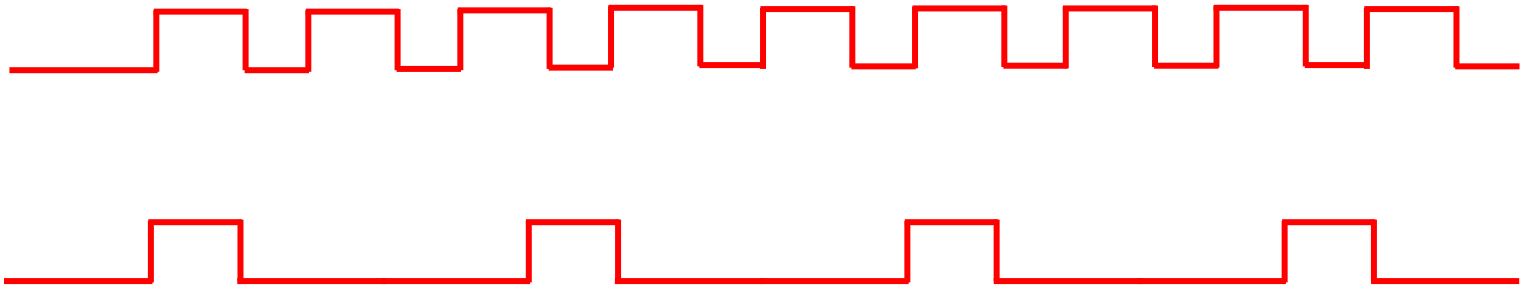




Let's pause for a minute

Observation

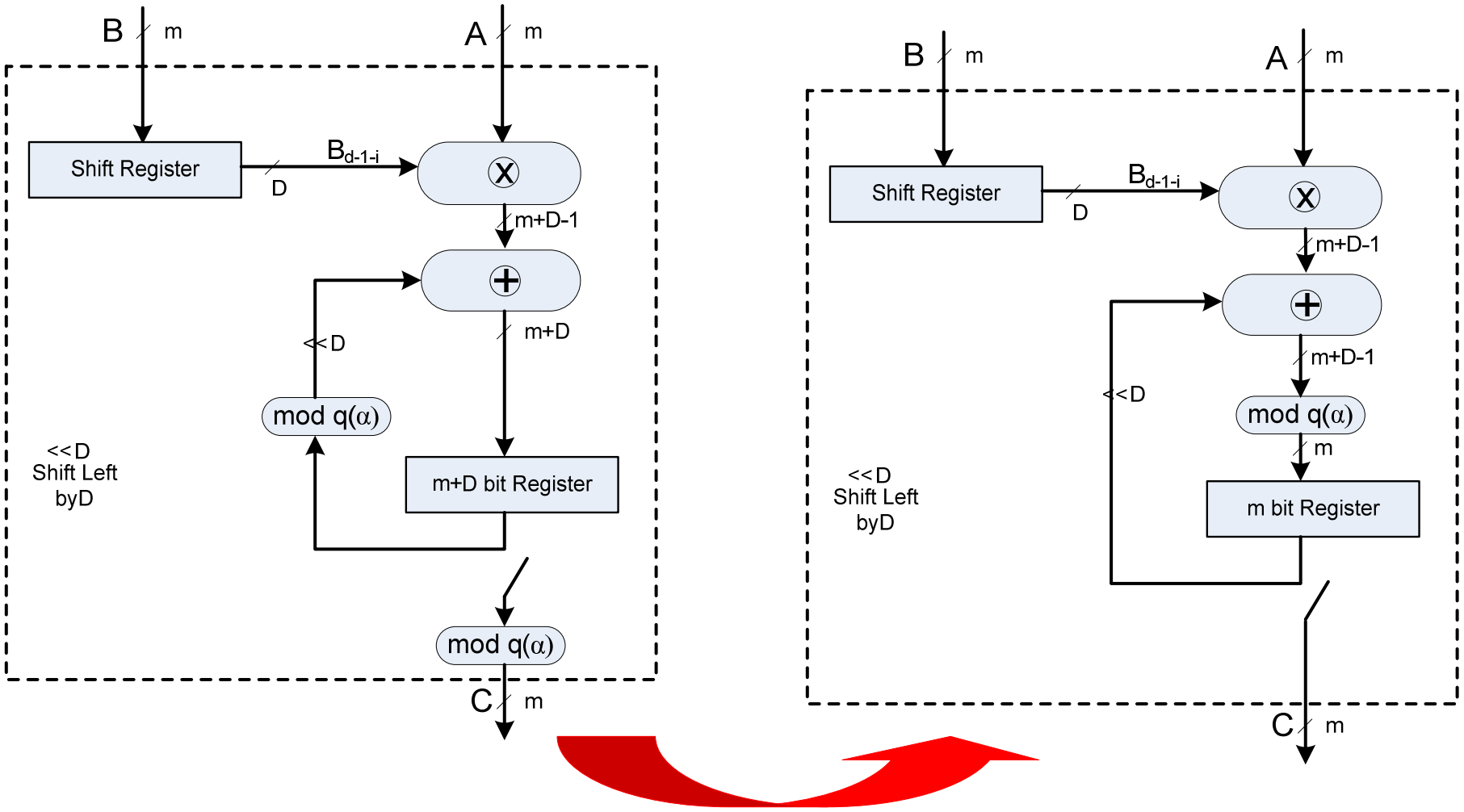
We are running at a very low frequency



Consequence

We do not have to do things in parallel to gain time!

Optimized MSDE Multiplier



Comparison

Source	AND	XOR	MUXex	Flip-Flops	Critical Path
Traditional LSDE	mD	D(m+2k+1)-(k+1)	m	3m+D-1	Log(D+1) T_{XOR} +T_{AND} + T_{MUX}
Traditional MSDE	mD	D(m+2k+1)-(k+1)	_	2m+D	Log(2D+1) T_{XOR} +T_{AND} + T_{MUX}
Batina et al. (ESAS 2006)	D(m+1)	D(m+k+1)	_	2m	2D T_{XOR} +T_{AND}
Optimized MSDE (This work)	mD	D(m+k)	-	2m	(Log(D)+Log(D+1)) T_{XOR} +T_{AND}

Contents

Conclusions

- New multiplier suited for ultra-low cost applications
- Future work, ecc implementation
- Take advantage of the low frequency of operation


PHILIPS