

RSA Hardware Research Ideas

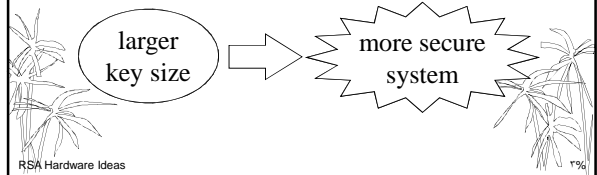


RSA Hardware Ideas

1%

RSA Security

* Security depends on the key size.



RSA Hardware Ideas

2%

RSA Public Key Cryptosystem

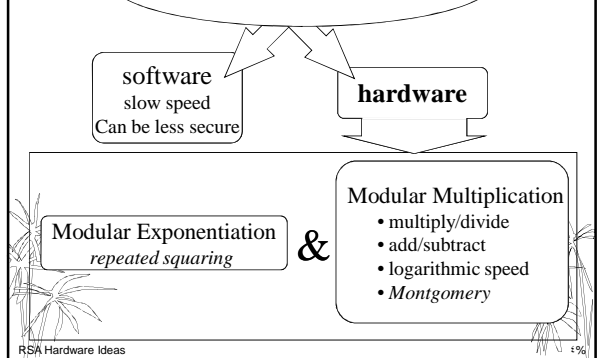
- Developed in 1978, by Rivest, Shamir & Adleman
- Its security is based on the *integer factoring problem*
- The most popular method :-
 - simple to understand & implement
 - same algorithm for encryption & decryption
 - can also be used for digital signature



RSA Hardware Ideas

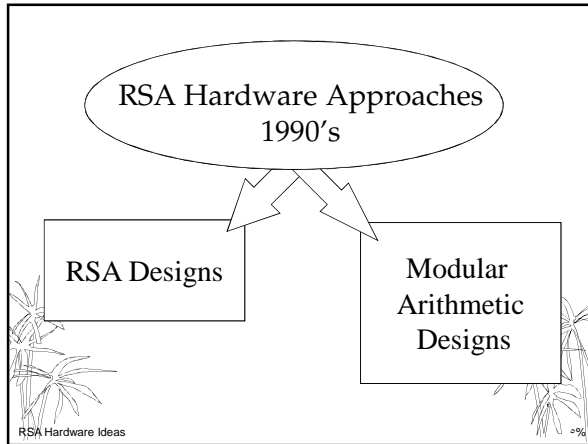
3%

RSA Implementations



RSA Hardware Ideas

4%

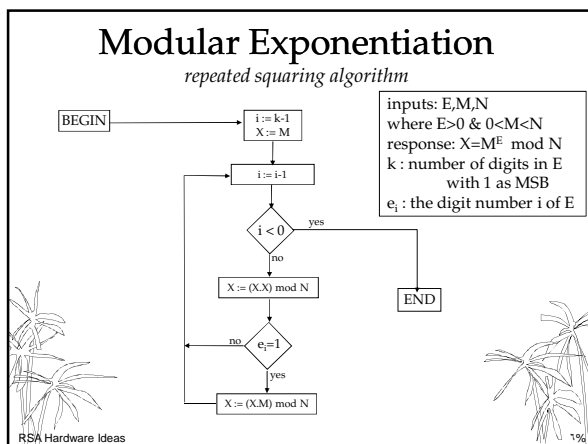


Modular Exponentiation Example

repeated squaring algorithm

- Compute: $3^9 \bmod 7$
- $k = 9 = (1001)_2$; $i = 3$; $X = M = 3$
 - $i = 2$; $X = 3.3 = 2$; $e_2 = 0 \Rightarrow X = 2$ (no change since $e_i = 0$)
 - $i = 1$; $X = 2.2 = 4$; $e_1 = 0 \Rightarrow X = 4$ (no change since $e_i = 0$)
 - $i = 0$; $X = 4.4 = 2$; $e_0 = 1 \Rightarrow X = 2.3 = 6$
- $3^9 \bmod 7 = X = 6$

RSA Hardware Ideas



Modular Exponentiation Example

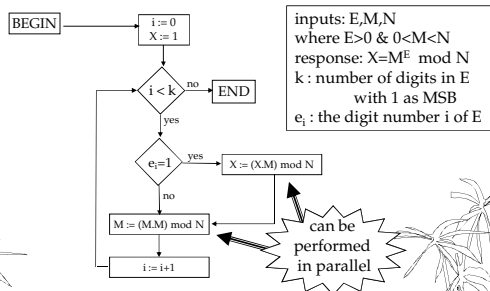
repeated squaring algorithm

- Compute: $7^{27} \bmod 10 = 3$
- $k = 27 = (11011)_2$; $i = 5$; $X = M = 7$
 - $i = 3$; $X = 7.7 = 9$; $e_3 = 1 \Rightarrow X = 7.9 = 3$
 - $i = 2$; $X = 3.3 = 9$; $e_2 = 0 \Rightarrow X = 9$ (no change since $e_i = 0$)
 - $i = 1$; $X = 9.9 = 1$; $e_1 = 1 \Rightarrow X = 1.7 = 7$
 - $i = 0$; $X = 7.7 = 9$; $e_0 = 1 \Rightarrow X = 9.7 = 3$

RSA Hardware Ideas

Modular Exponentiation

improved repeated squaring



RSA Hardware Ideas

Modular Exponentiation Example

improved repeated squaring algorithm

- Compute: $7^{10} \bmod 10 = 9$
- $k = 10 = (1010)_2$; $i = 0 \rightarrow 3$; $X = 1$; $M = 7$
 - $i = 0$; $e_0 = 0 \Rightarrow X = 1$ (no change since $e_i = 0$); $M = 7.7 = 9$
 - $i = 1$; $e_1 = 1 \Rightarrow X = 1.9 = 9$; $M = 9.9 = 1$
 - $i = 2$; $e_2 = 0 \Rightarrow X = 9$ (no change since $e_i = 0$); $M = 1.1 = 1$
 - $i = 3$; $e_3 = 1 \Rightarrow X = 9.1 = 9$; $M = 1.1 = 1$

RSA Hardware Ideas

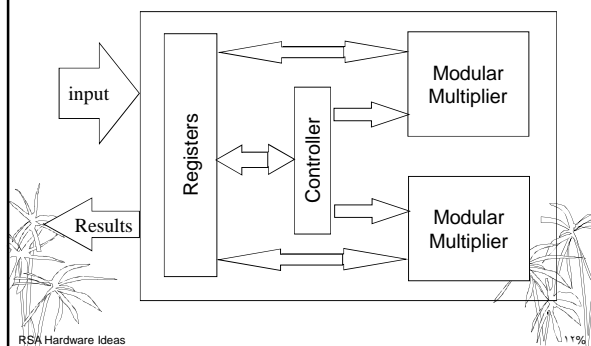
Modular Exponentiation Example

improved repeated squaring algorithm

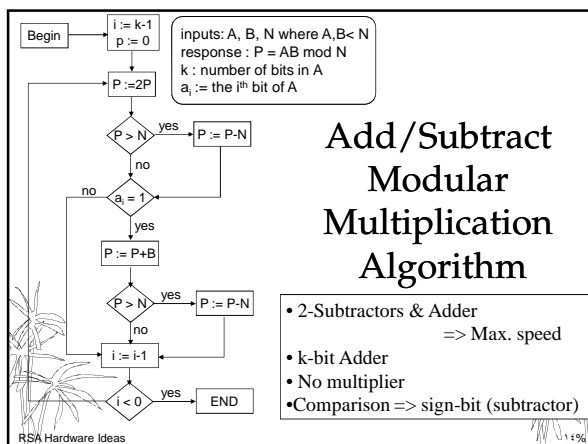
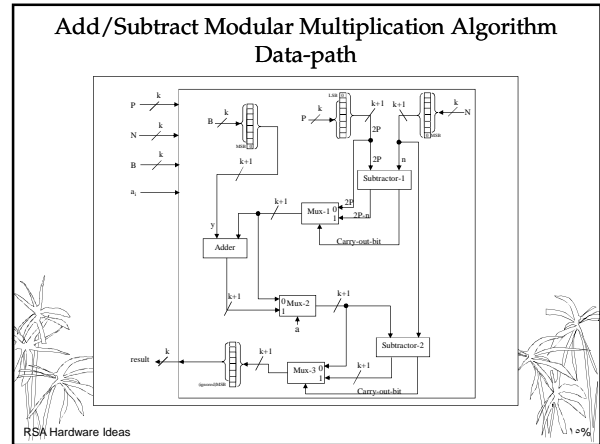
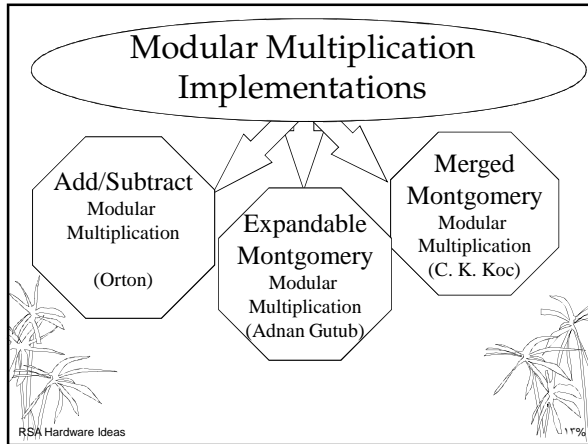
- Compute: $3^9 \bmod 7$
- $k = 9 = (1001)_2$; $i = 0 \rightarrow 3$; $X = 1$; $M = 3$
 - $i = 0$; $e_0 = 1 \Rightarrow X = 1.3 = 3$; $M = 3.3 = 2$
 - $i = 1$; $e_1 = 0 \Rightarrow X = 3$ (no change since $e_i = 0$); $M = 2.2 = 4$
 - $i = 2$; $e_2 = 0 \Rightarrow X = 3$ (no change since $e_i = 0$); $M = 4.4 = 2$
 - $i = 3$; $e_3 = 1 \Rightarrow X = 3.2 = 6$; $M = 2.2 = 4$
- $3^9 \bmod 7 = X = 6$

RSA Hardware Ideas

Modular Exponentiation Hardware



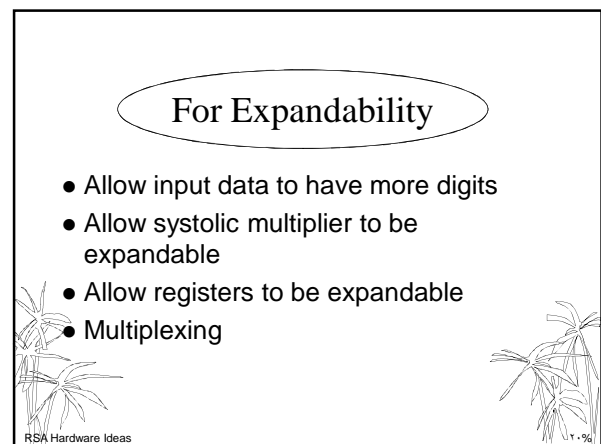
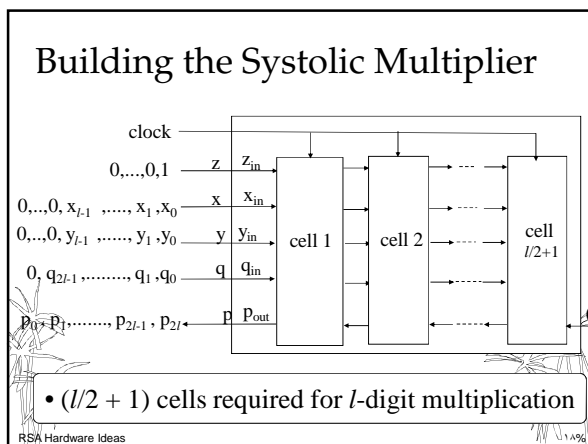
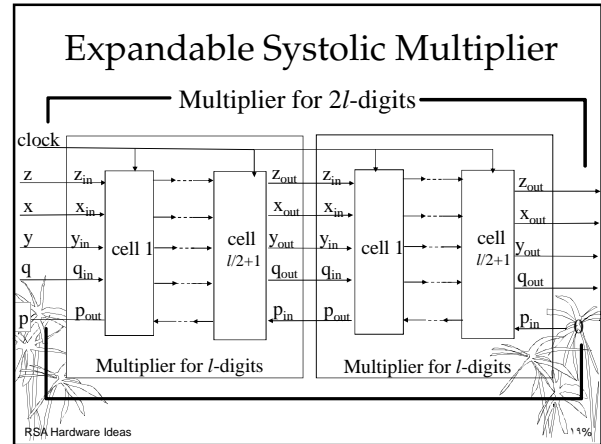
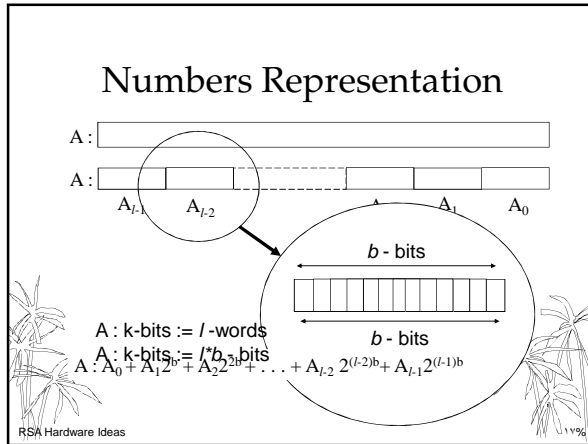
RSA Hardware Ideas

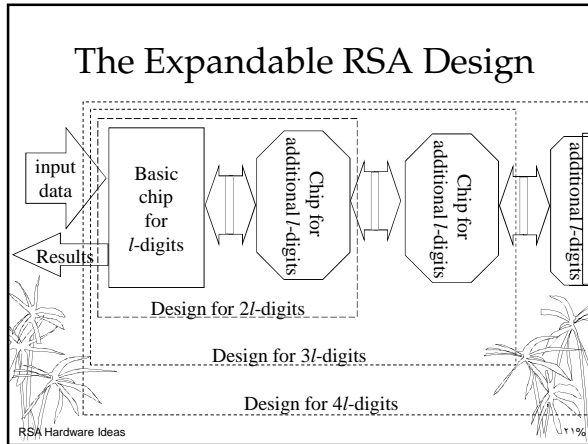


Expandable RSA Hardware

- Crypto Hardware is faster & more secure compared to software
- However, it is limited by its design parameters and capability.
- If more security is needed & more bits are needed to be computed, a new hardware is to be designed and the old one cannot be utilized.
- Expandable hardware will be flexible to solve this problem by adding extra chips whenever needed.

RSA Hardware Ideas





Expandable RSA Hardware Ideas Summary

- The expandable hardware has the best speed while its area is the largest.
- The add/subtract model has the best area while its speed is the slowest.
- The cost ($\text{Area} \times \text{Time}^2$) of the merged design is the best followed by the expandable design, and then the add/subtract model.

RSA Hardware Ideas