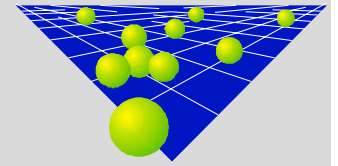
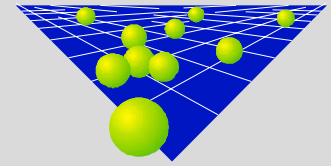


# Aspects of Public Key Cryptosystems in Practice

Erwin Hess  
SIEMENS AG  
Corporate Technology  
Munich, Germany



# RSA or Elliptic Curves ?



## The Current Status of Public Key Cryptography (I)

### ■ RSA

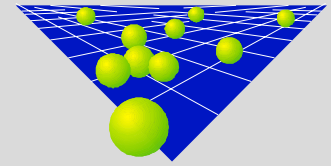
still the most popular public key system

#### ◆ Pro's:

- easy to understand - even for non-experts
- easy to implement
- patent expired
- underlying mathematical problem considered "old" and hard

#### ◆ Contra's:

- extra-long parameters
- multiplicativity
- vulnerable again side-channel-attacks



## The Current Status of Public Key Cryptography (II)

### ■ Elliptic Curves

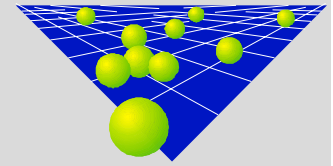
the most attractive alternative to RSA

#### ◆ Pro's:

- shorter parameters
- shorter digital signatures
- faster than RSA
- cryptographic security grows exponentially with length of parameters

#### ◆ Often heard Contra's:

- underlying mathematical problem considered "new"
- confusing patent situation
- confusing number of implementation options
- more difficult to explain and to implement



## Side Channel Attacks - SPA and Timing Attack

### ■ SPA: Simple Power Attack

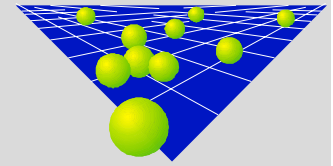
- ◆ Attack: *Direct interpretation of power consumption measurement.*
- ◆ Defense: *Avoid key dependent power profile by uniforming the computations*

### ■ Timing Attack:

- ◆ Attack: *Statistical evaluation of the correlation between key bits, plaintext and the running time of the cryptographic algorithm*
- ◆ Defense: *Make running time independent of key bits by uniformization of the computations. Randomize input and/or keybits*

### ■ Methods to protect EC cryptosystems against SPA and timing attacks:

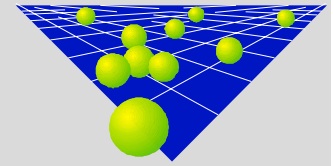
- ◆ Use Montgomery's method for point multiplication
- ◆ Introduce dummy operation to "homogenize" the point operations
  - $P \rightarrow P + P$
  - $P, Q \rightarrow P + Q$



## Side Channel Attacks - DFA and DPA

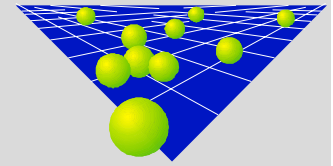
It seems that elliptic curve based cryptosystems are easier to protect against DFA and DPA than the RSA-system.

- DFA: Differential Fault Analysis
  - ◆ Attack: *Induce computational errors to the device and deduce key bits from the information leaked by the faulty result*
  
  - ◆ Defense: *Check the consistency of the result of computation*
    - RSA: Complicated protocols with additional consistency relations.
      - Shamir's protection against the Bellcore-attack
  
    - EC: Consistency relation is implicitly given.
      - Check if resulting point is on curve.



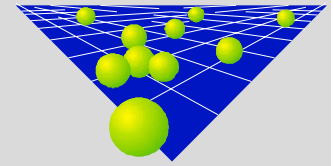
## Side Channel Attacks - DFA and DPA (II)

- DPA      *Differential Power Analysis*
  - ◆ Attack:      Apply statistical tests to intermediate results in order to detect correlations between and plain-/ciphertext in the power consumption profile.
  
  - ◆ Defense:      Decorrelation of intermediate results and key-bits, plain- and ciphertext by randomization.
    - RSA:      Randomize exponent and/or basis of modular exponentiation.
  
    - EC:      As in the case of RSA, and use randomized projective coordinates.



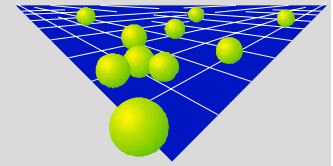
## Side Channel Attacks - Consequences

- It seems that elliptic curve based cryptosystems can be protected against DFA and DPA with less additional costs than RSA.
  
- Implementation of the RSA-system is getting more complicated
  - ◆ randomization
  - ◆ consistency checks
  
- One might expect that RSA is rapidly losing its attractiveness.



## Basic Constituents for Elliptic Curve Based Cryptosystems

- Cryptographic schemes
  - ◆ easily derived from the the classical DL-schemes in  $GF(p)^*$ 
    - EC-DH, EC-DSA, etc.
- Good curves
  - ◆ now in a sufficient way under control
    - CM-curves with large class number (Spallek, Morain, Lay)
    - SEA-algorithm (Schoof, Atkin, Elkies, Müller, Couveigne, Lercier)
- Random number generator
  - ◆ Crucial cryptographic operation for most schemes  $k, P \rightarrow [k] \cdot P$   
(k is a random integer, P a point on an elliptic curve, k to be used only once)
- Arithmetic support
  - ◆ field arithmetic in the underlying finite field
  - ◆ ordinary modular arithmetic (modulo the group order of a point P)



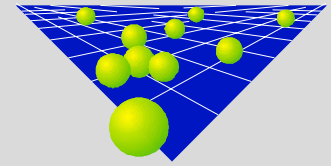
## Today's Options for Elliptic Curve Based Cryptosystems (I)

The current standards for elliptic curve based cryptosystems offer a (unnecessary ?) large number of implementation options:

- ◆ various schemes for the same cryptographic mechanism
- ◆ various choices for the underlying finite field
  - $GF(p)$
  - $GF(2^n)$ 
    - normal basis representation
    - polynomial basis representation
  - $GF(p^n)$       binary length of  $p \sim$  word length of chosen processor

**consequence**

We are losing the common arithmetic basis of public key cryptography



## Options for Elliptic Curve Based Cryptosystems (II)

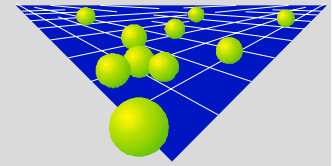
Elliptic curves defined over prime fields  $GF(p)$

Pro's:

- ◆ Based on ordinary modular arithmetic
- ◆ Dual mode with RSA possible
- ◆ Offers migration path for RSA-users
- ◆ One more "degree of freedom"

Often heard Contra's:

- ◆ Impossible on smart cards
- ◆ Area consumption too large
- ◆ Much slower than elliptic curves over  $GF(2^n)$



## Options for Elliptic Curve Based Cryptosystems (III)

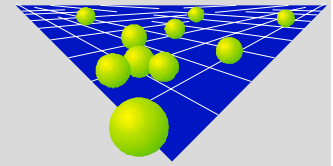
Elliptic curves defined over prime fields  $GF(2^n)$

Pro's:

- ◆ Arithmetic is easy to implement
- ◆ Can be run with very high clock frequency
- ◆ Area and power consumption smaller than in the case of  $GF(p)$

Contra's:

- ◆ The use of ordinary modular arithmetic cannot be avoided
- ◆ High clocking rate cannot be used in smart cards
- ◆ Patent situation
  - The idea to implement arithmetic units for  $GF(2^n)$  and  $\text{mod}(N)$  on **one** IC might be covered by a patent.



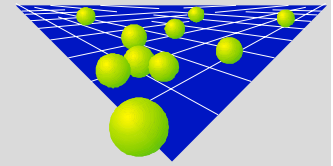
## Elliptic Curve Cryptosystems - Patent Situation

- The general idea to use elliptic curves for public key cryptosystems is free of patents
- All the relevant public key based security services
  - ◆ digital signatures, key exchange, authenticationcan be realized in a patent free way

### BUT:

- Some elliptic curve analogues of cryptographic schemes are covered by patents
  - ◆ Menezes-Qu-Vanstone, Nyberg-Rueppel, Schnorr, etc.
- There is a large number of patents covering special implementation techniques

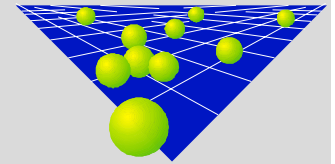
## Unpleasant Experiences with Elliptic Curve based Cryptosystems



- Some ideas to make implementations of elliptic curve based cryptosystems faster or easier to implement turned out to be counterproductive.
  - ◆ Use of supersingular curves
    - Idea: Avoid determining the number of points
  - ◆ Use of anomalous curves
    - Idea: Double use of arithmetic
  - ◆ Use of curves over  $GF(2^{mn})$ 
    - Idea: Store parts of the arithmetic



**Avoid unnecessary fixings**



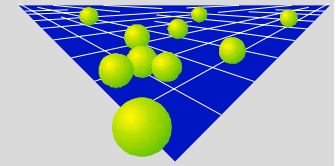
## Hardware Supporting Elliptic Curve Cryptosystems

### INFINEON:

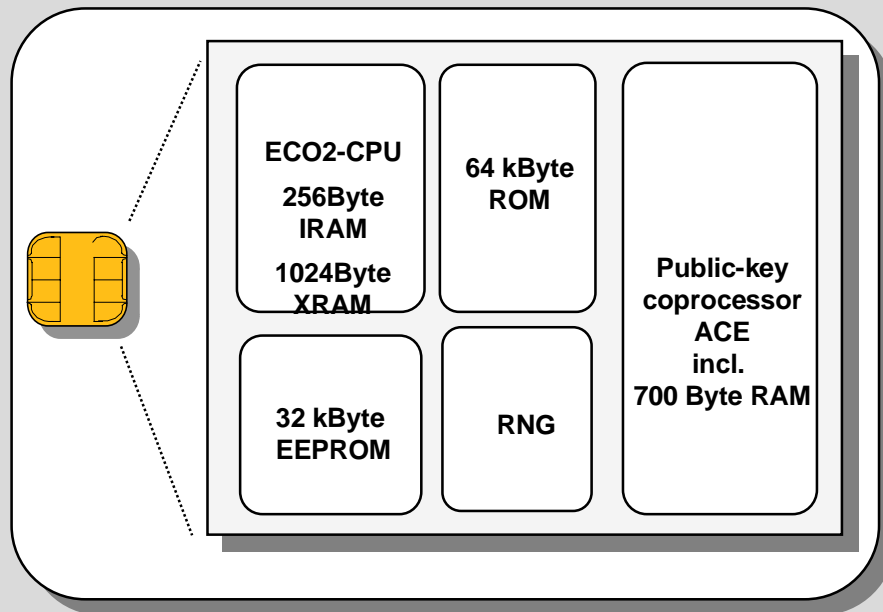
- The Smart Card-ICs SLE66CxxP
  - ◆ A family of smart card ICs supporting public key algorithms based on ordinary modular arithmetic.

### SIEMENS:

- The PLUTO-IC
  - ◆ A high-performance encryption IC. (encryption rate 2Gbit/sec)
  - ◆ Elliptic curve cryptosystem based on curves over  $GF(p)$ ,  $p$  of length 320 bit
  
- ELCRODAT-6-2
  - ◆ An encryption device for the ISDN-telecommunication network
  - ◆ Elliptic curve cryptosystem based on curves over  $GF(p)$ ,  $p$  of length 256 bit

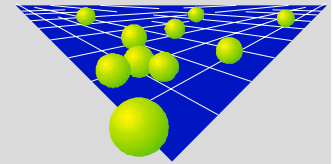


## The Infineon Smart-Card-IC SLE66CX320P

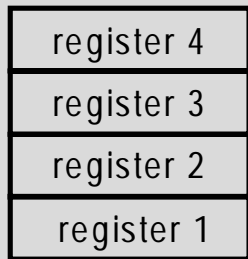


- Public key coprocessor for modular arithmetic
- True physical random number generator
- Support of RSA and elliptic curves over GF(p)
  - ◆ RSA: up to 1024 Bit
  - ◆ Elliptic curves: up to 256 Bit
- Dedicated 700 Bytes of Crypto RAM
- Architecture optimized for minimum power consumption
- maximum clock frequency: 15 MHz
- Total area of public key coprocessor:

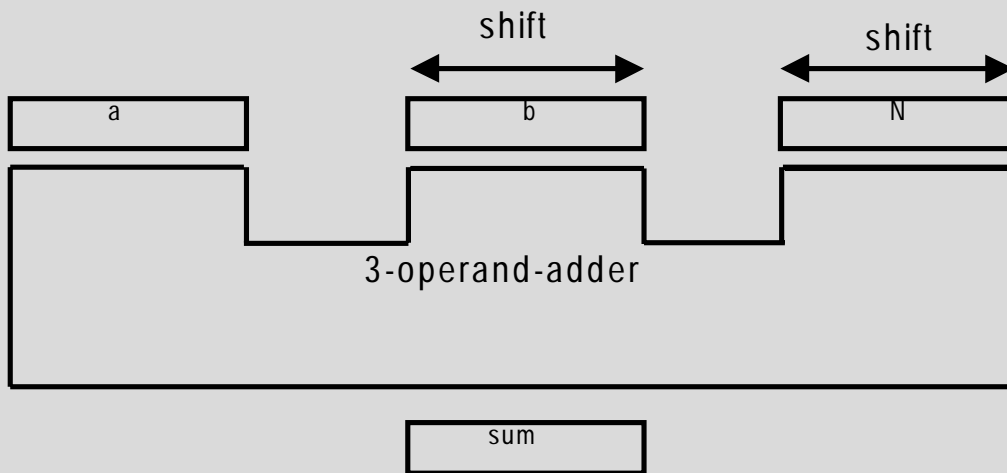
**<< 1mm<sup>2</sup>** (0.25μ technology)



# The Public Key Coprocessor of SLE66CxxP

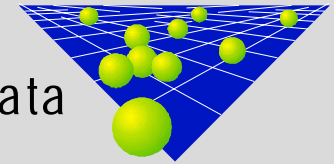


not optimized for EC-support



## Characteristics:

- ◆ 3-operand-parallel-adder
- ◆ parallel/serial multiplication
- ◆ Booth's algorithm to reduce the number of partial products
- ◆ special modular reduction based on an comparing with  $(2/3) \cdot N$
- ◆ 4 registers of length 560 bit
- ◆ execution time for one modular multiplication of n-bit-integers:  
 $(1/2.8) \cdot n$  clock cycles



## The Infineon Smart-Card-IC SLE66CX320P - Performance Data

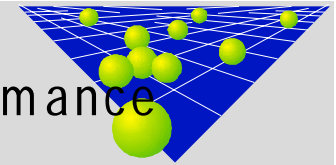
Operation	[length of modulus]	execution time [@15 MHz]
[k]P on EC over GF(p)	160 bit	83 ms
[k]P on EC over GF(p)	256 bit	234 ms
$a^b \bmod N$	1024 bit	220 ms



Elliptic curves are faster than RSA, even on devices optimized for RSA-support

### Elliptic curves on SLE66:

- All curves of type  $y^2 = x^3 + ax + b$  over GF(p) are possible
- No restrictions concerning the parameters a, b and p
- Points P and [k]P in affine representation
- Calculation of [k]P using projective co-ordinates
- Patent-free implementation



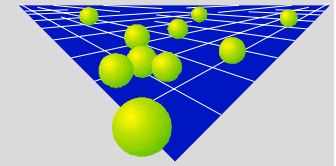
## The Infineon Smart-Card-IC SLE66CX320P - Possible Performance

Operation	[length of modulus]	execution time [@15 MHz]
[k]P on EC over GF(p)	160 bit	83 ms
[k]P on EC over GF(p)	256 bit	234 ms
$a^b \bmod N$	1024 bit	220 ms

← < 15 ms  
← < 35 ms

Expected performance under the conditions

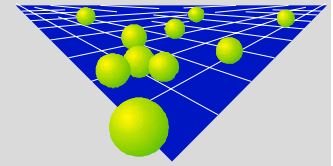
- Register organization optimized for EC-support
- Fast modular division available



## The Encryption Device ELCRODAT 6-2



- ED 6-2S for the Euro-ISDN basic rate interface ( $S_0$ )
  - ◆ different line configurations:
    - point-to-point, e.g. interfacing of PBX
    - passive bus, up to eight subscribers (TE)
  - ◆ two independent B-channels
  
- ED 6-2M for the Euro-ISDN primary rate interface ( $S_{2M}$ )
  - ◆ connection of PBX via  $S_{2M}$ -Interface
  - ◆ 30 independent B-channels
  
- Common Features of ED 6-2M and ED 6-2M
  - ◆ Tempest proof
  - ◆ Evaluated up to "TOP SECRET"
  - ◆ remote certificate update

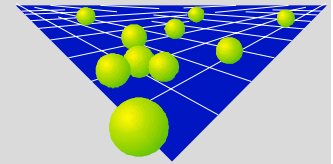


## ELCRODAT 6-2 -Cryptographic Features

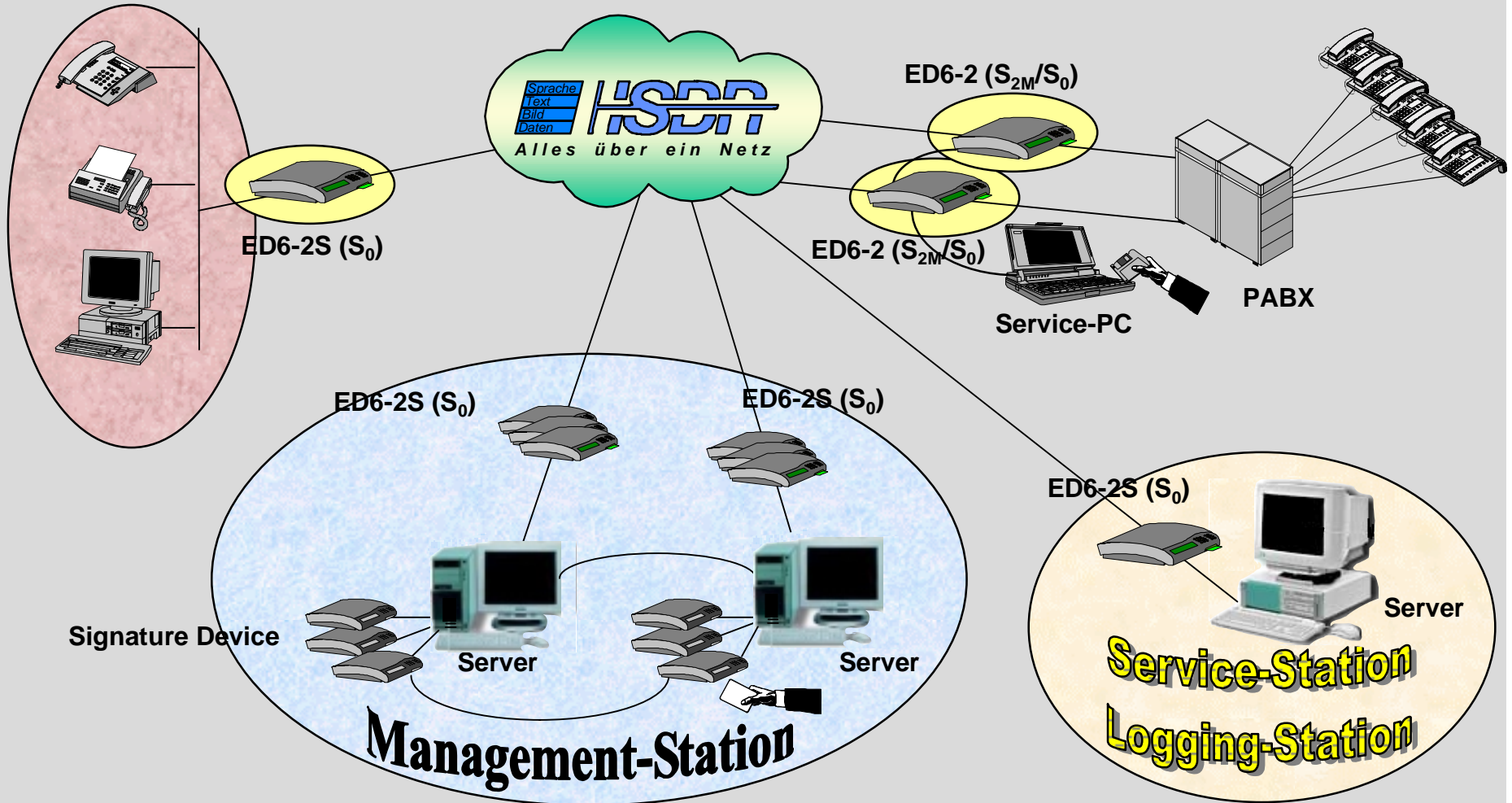


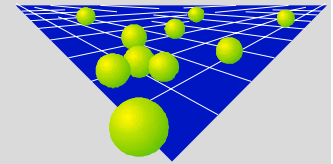
- Public Key System, based on elliptic curves over  $GF(p)$ 
  - ◆ Size of  $p$ : 256 Bits
  - ◆ digital signatures, authentication, key exchange
  - ◆ Certificates, based on X.509
- Hash function RIPE MD-160
- Access protection with smart card
- Physical random number generator
- Symmetric encryption algorithm
- Each ED 6-2 supports up to 1024 closed user groups
  - ◆ 32 different Management Groups (separate certificates and separate cryptographic parameters), each consists of up to 32 separate compartments



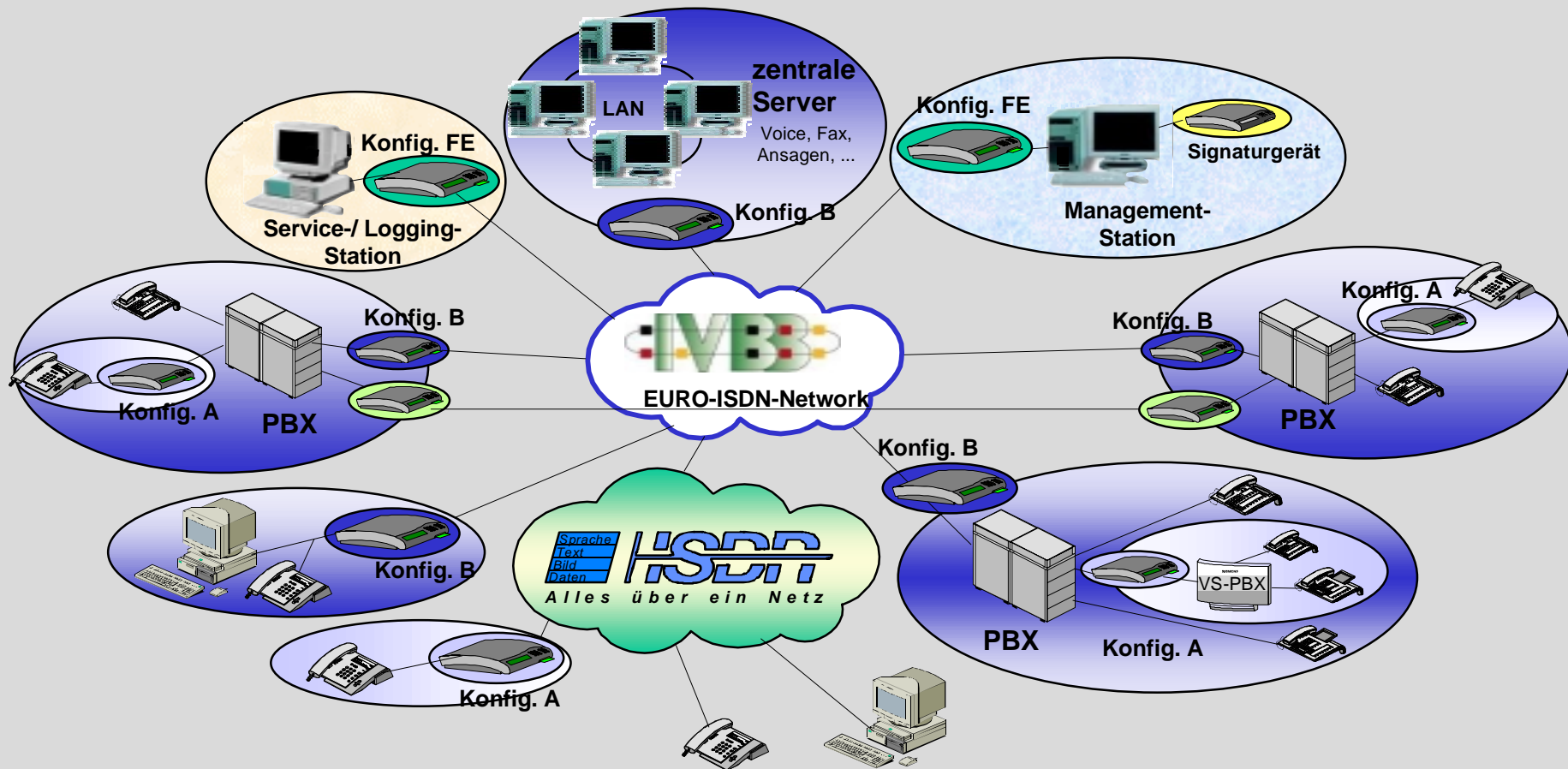


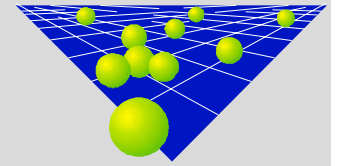
# ELCRODAT 6-2 - Overview





# Use of ELCRODAT 6-2 in the German Government Network IVBB





## Conclusion

### **Elliptic curve cryptography is a mature technology**

- All the necessary components are available
- Systems are already in practical use
- Patent free approach is possible



**Why do you still hesitate to move towards elliptic curve cryptography?**