Signcryption ---
The Road to an International Standard

Yuliang Zheng

University of North Carolina at Charlotte

yzheng@uncc.edu

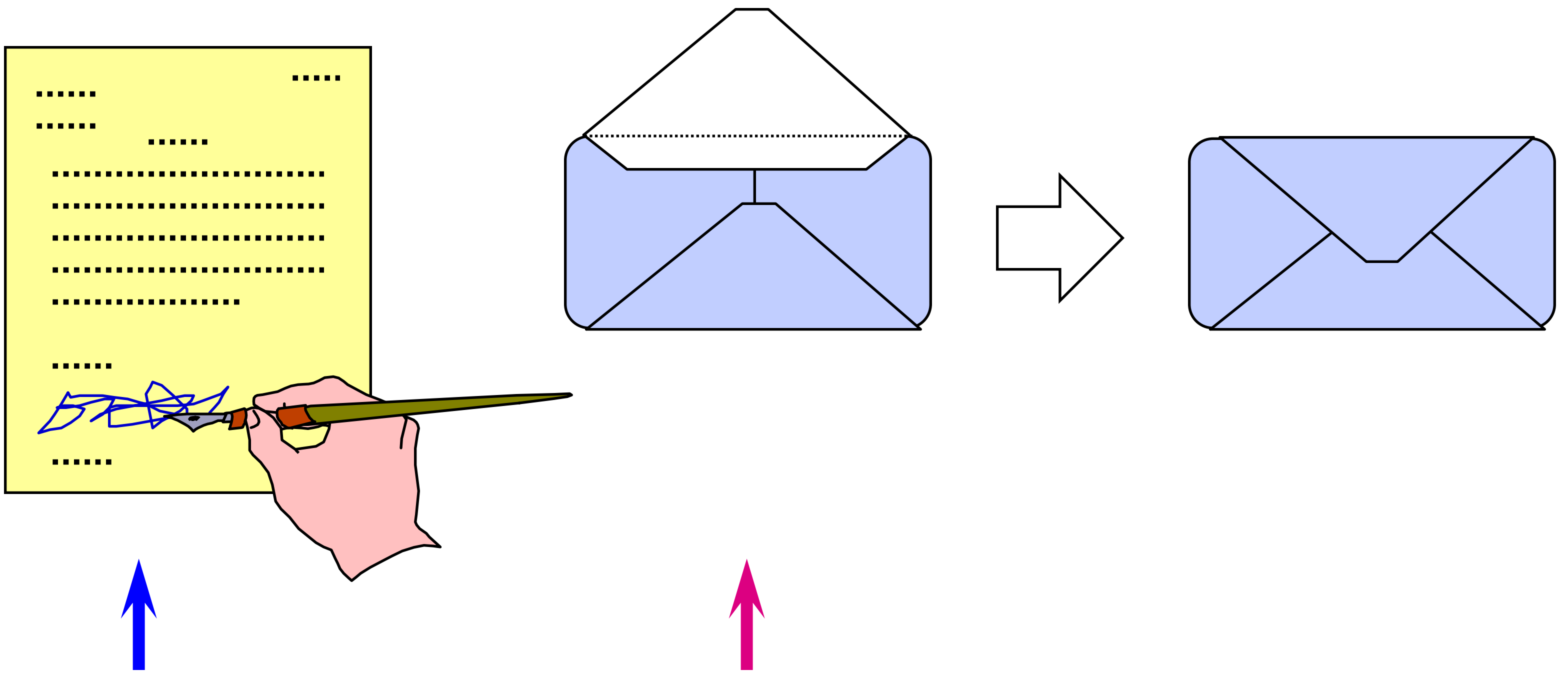
July 31, 2013

Objectives of Cyber Security

Goals of Cryptography: C + I

- Confidentiality
  - Symmetric/private key encryption
  - Asymmetric/public key encryption
- Integrity & Authenticity
  - Trusted parties --- symmetric/private key authentication
  - Untrusted parties --- asymmetric/public key authentication (digital signature, unforgeability)
- Minimizing cost/overhead
  - Less computation (over large integers)
  - Smaller expansion in length
    (= less communication overhead)
  - Especially important for smartphones & portable devices w/ limited battery life

In the Paper & Ink World:
Signature followed by Seal

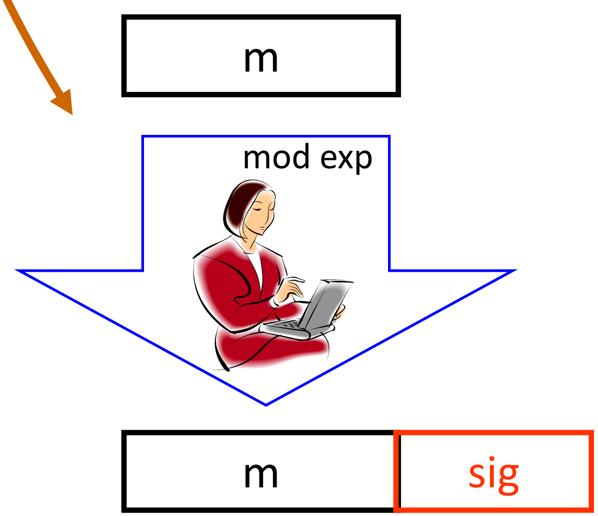


To achieve:
authenticity
(unforgeability &
non-repudiation)

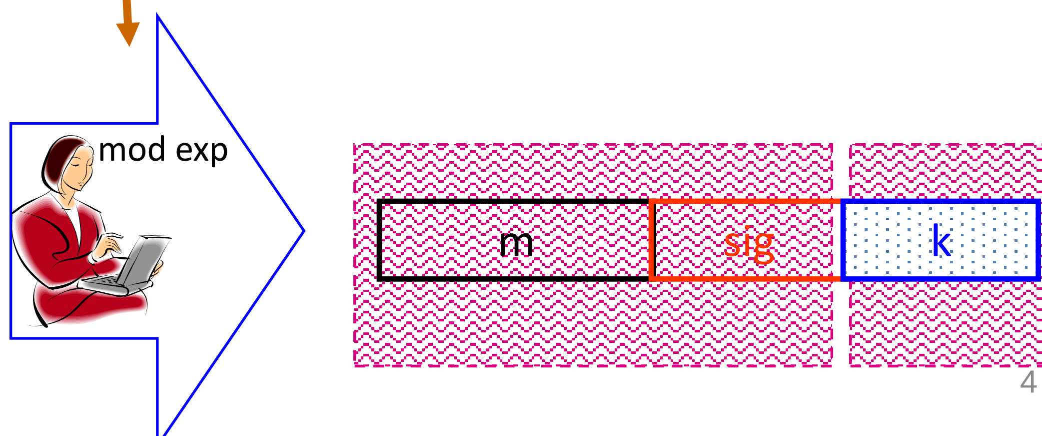
To achieve:
confidentiality

In the Digital World:
Digital Signature followed by Encryption

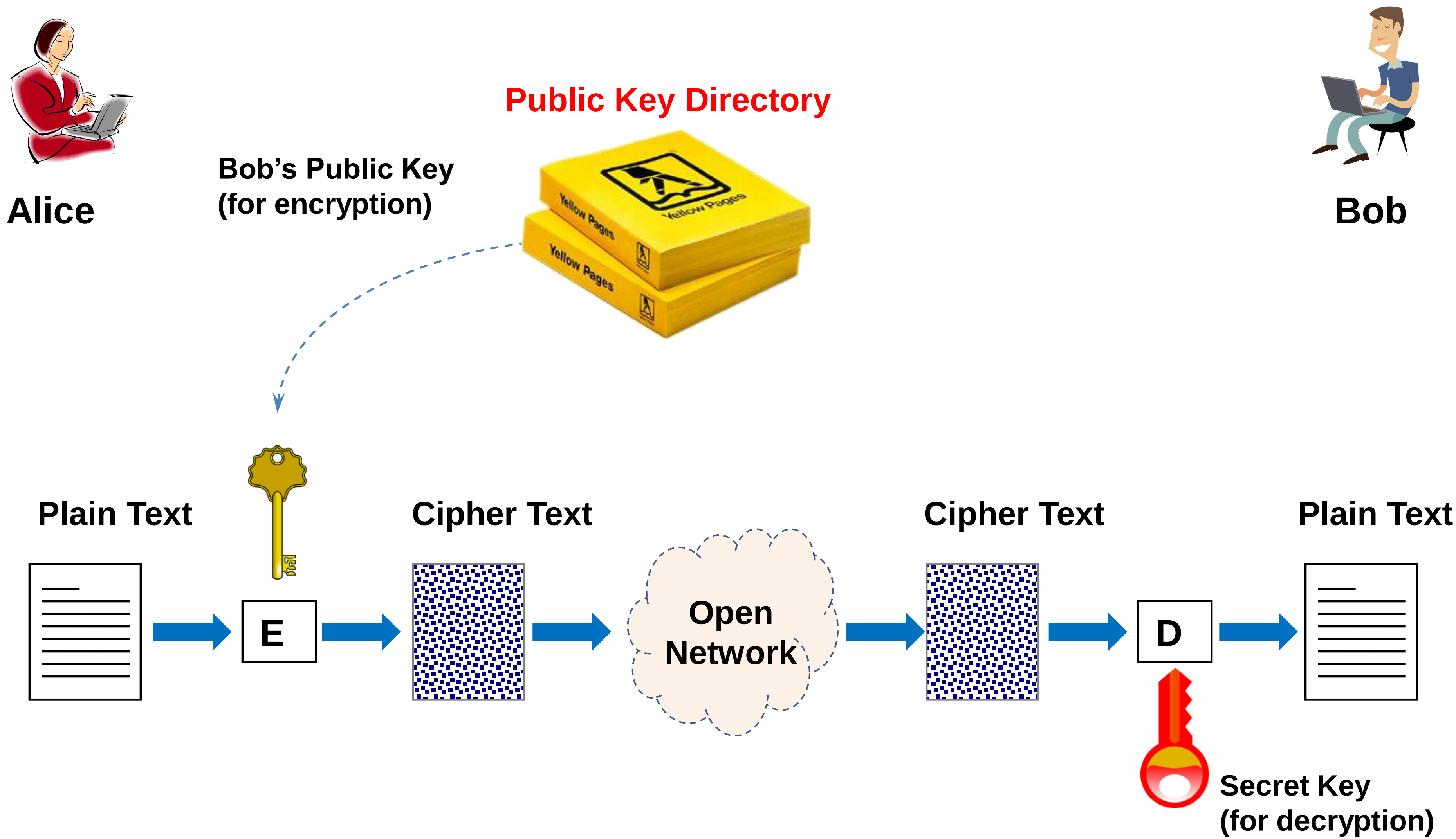
- **Step 1 --- Add Signature**
  - **Alice the sender signs a message *m* using her secret key, i.e. creating *sig* on *m*.**



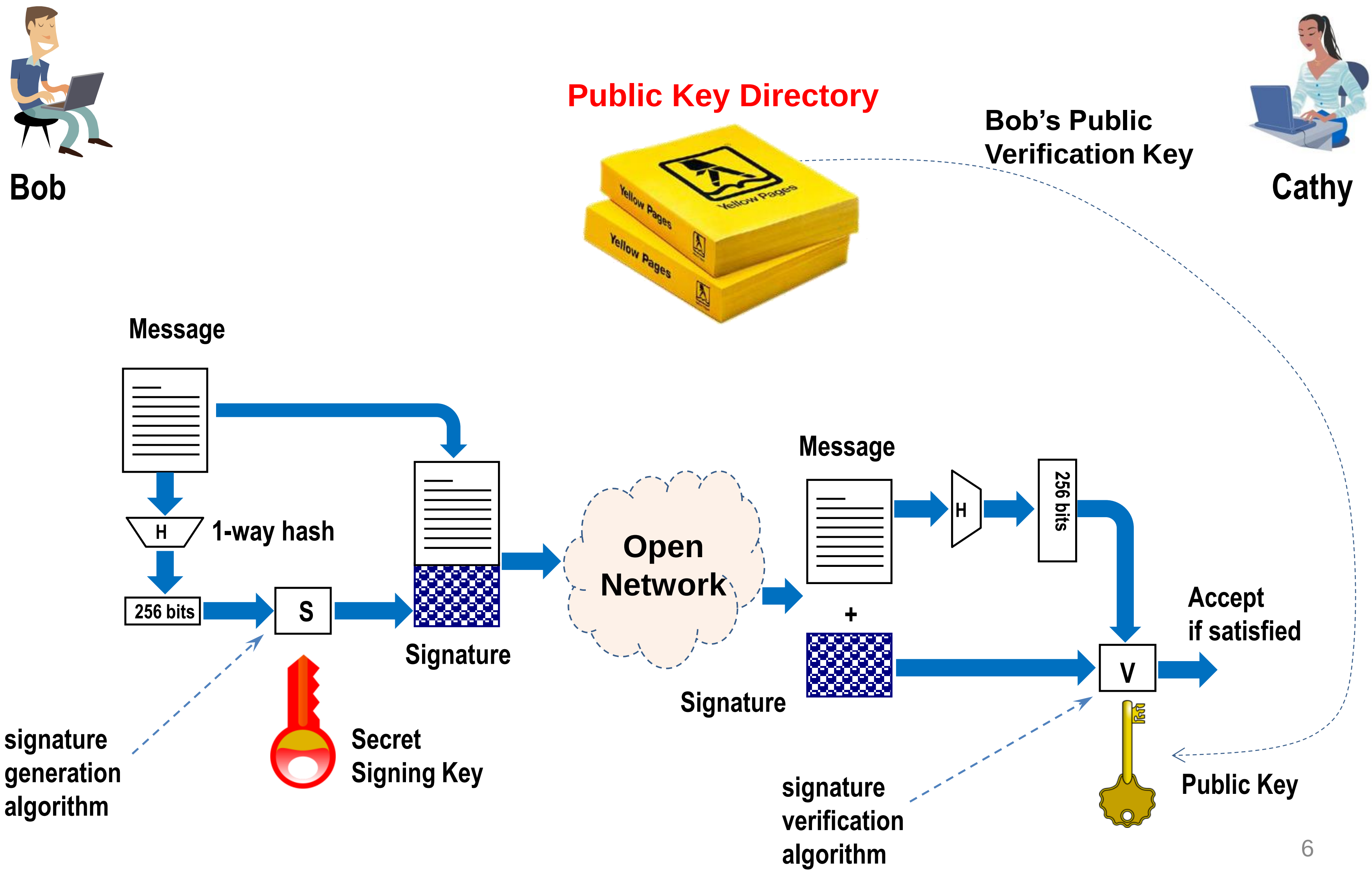
- **Step 2 --- Do Encryption**
  - **Alice encrypts (*m*,*sig*) using AES with a random key *k*.**
  - **Alice encrypts *k* using Bob's public key.**



Public Key Encryption



Public Key Digital Signature



Notable Public Key Techniques

Public Key Encryption

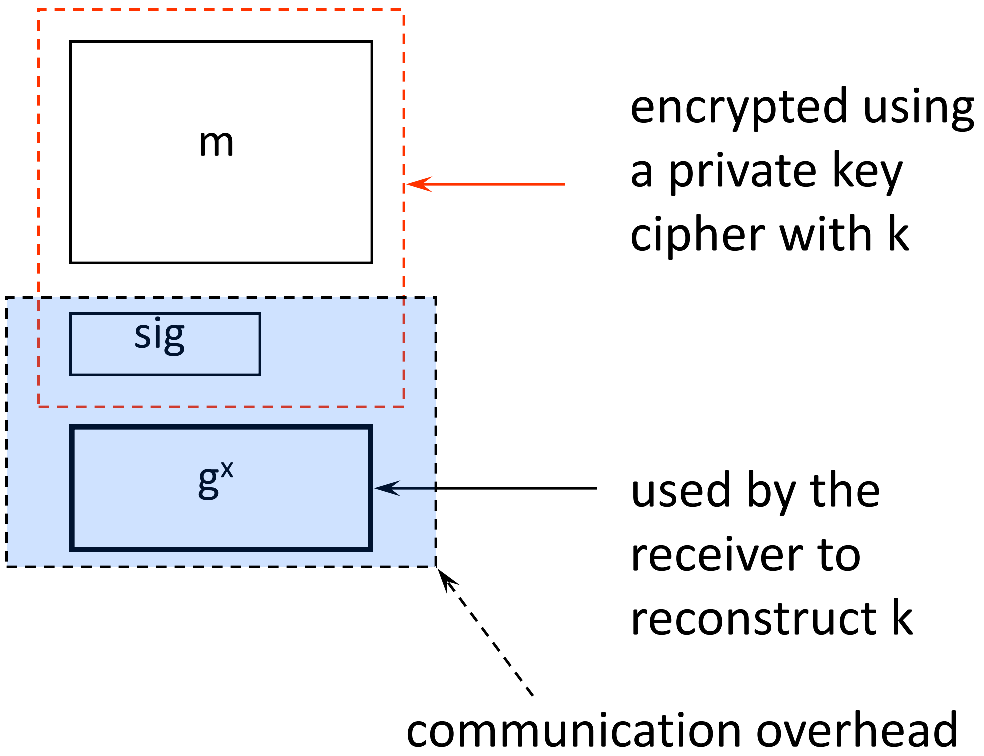
- Factorization based
  - RSA encryption
  - Rabin
- Discrete log based
  - Diffie-Hellman
  - ElGamal encryption
  - Elliptic curve versions
- Lattice based
  - NTRU encryption

Digital Signature

- Factorization based
  - RSA signature
- Discrete log based
  - ElGamal signature
  - DSA (US standard)
  - Schnorr
  - Elliptic curve versions
- Lattice based
  - NTRU signature

Signature-then-Encryption (based on Discrete Logarithm)

EXP=3+2.17



Cost of Signature-then-Encryption

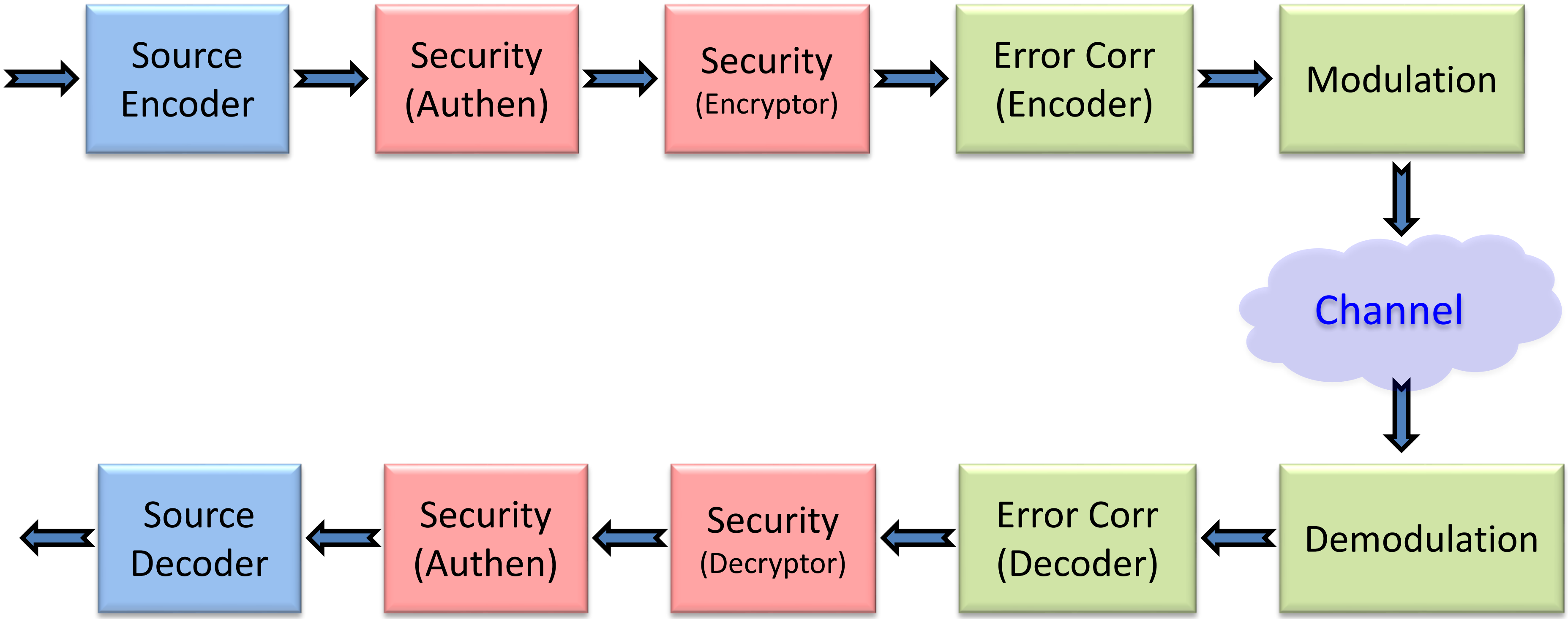
Schemes \ Cost	Comp Cost (No. of exp)	Comm Overhead (bits)
RSA based sig-then-enc	2 + 2	$\|n_a\| + \|n_b\|$
DL based Schnorr sig + ElGamal enc	3 + 2.17 (3 + 3)	$\|hash\| + \|q\| + \|p\|$

Both techniques require very high overhead!
(your smartphone's battery runs out fast!)

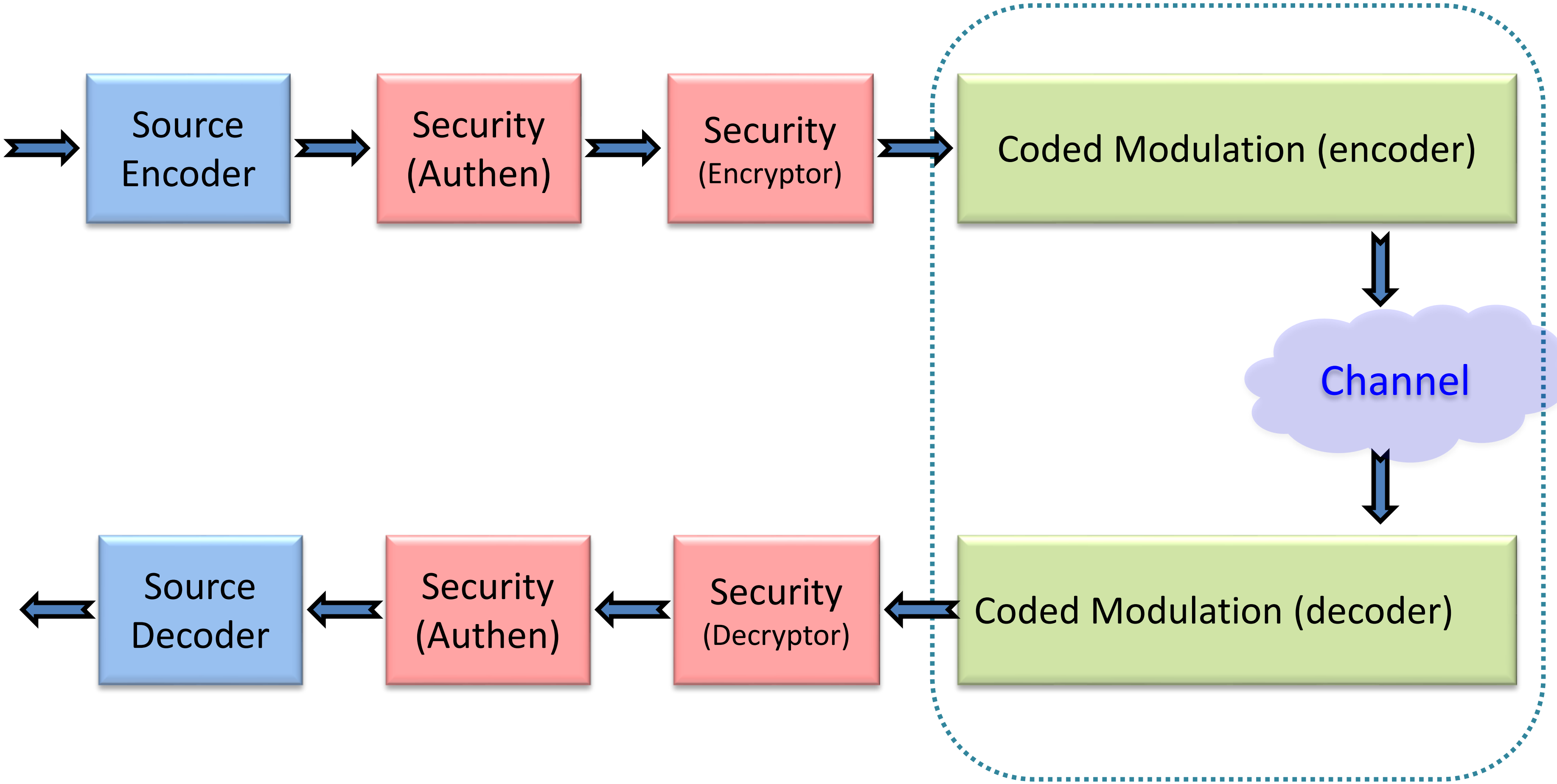
Improving Efficiency

- Can we do better than “signature followed by encryption” ?
  - For resource-constrained applications
    - Wireless mobile devices
    - Smart card applications
- Can we learn from other disciplines such as
  - Coded modulation in communications (= error correcting codes + modulation)
    - Imai-Hirakawa block coded modulation
    - Ungerboeck trellis coded modulation

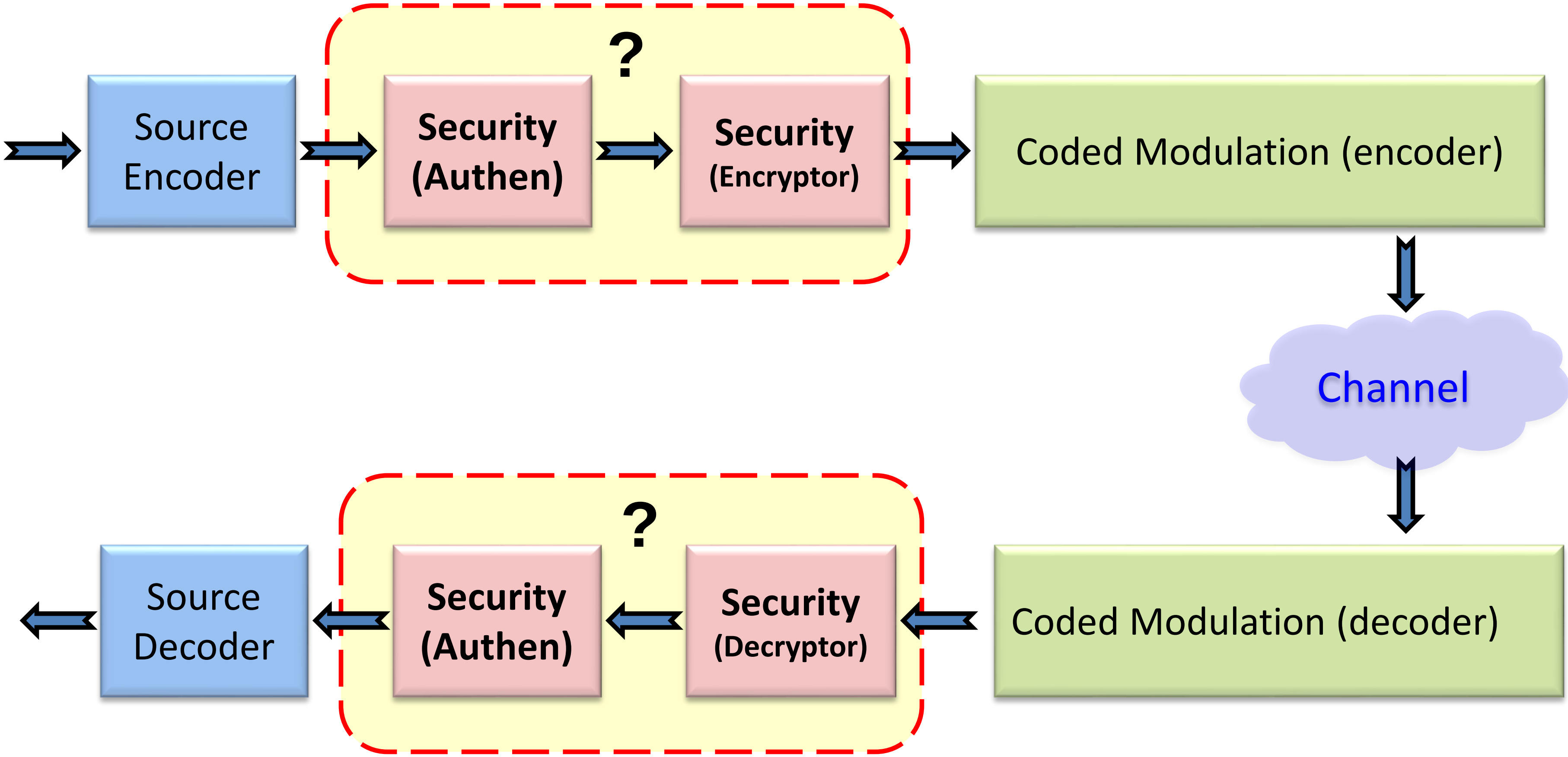
Communications System



Coded Modulation
--- one of the hottest in 80's



Co-Design of Digital Signature and Public Key Encryption ?



Goal: Signcryption (1996 @ Monash)

- To achieve both
  - confidentiality
  - authenticity
    - unforgeability &
    - non-repudiation
- With a <u>significantly smaller</u> comp. & comm. overhead:

Cost (signcryption) << Cost (signature) + Cost (encryption)

Signcryption -- Public & Private Parameters

- **Public to all**
  - *p* : a large prime
  - *q* : a large prime factor of *p-1*
  - *g* : *0<g<p* & with order *q* mod *p*
  - Two 1-way hash functions:
    - $G: \{0,1\}^* \rightarrow \{0,1\}^{256}$
    - $H: \{0,1\}^* \rightarrow Z_q$
  - (*E*,*D*) : private-key encryption & decryption algorithms, with 256-bit keys

- **Alice's keys**
  - Private key: $x_a \in_R Z_q$
  - Public key: $y_a = g^{x_a} \bmod p$

- **Bob's keys**
  - Private key: $x_b \in_R Z_q$
  - Public key: $y_b = g^{x_b} \bmod p$

Signcryption Algorithm

Signcryption by Alice:

$m \Longrightarrow (c, r, s)$

- Pick $x \in_R \{1, 2, \ldots, q-1\}$
- $T = {y_b}^x \bmod p$
- $r = H(T, m, y_a, y_b)$
- If $r + x_a = 0 \bmod q$, then start over again
- $s = \frac{x}{r + x_a} \bmod q$
- $k = G(T, y_a, y_b)$
- $c = E_k(m)$
- Send (c, r, s) to Bob

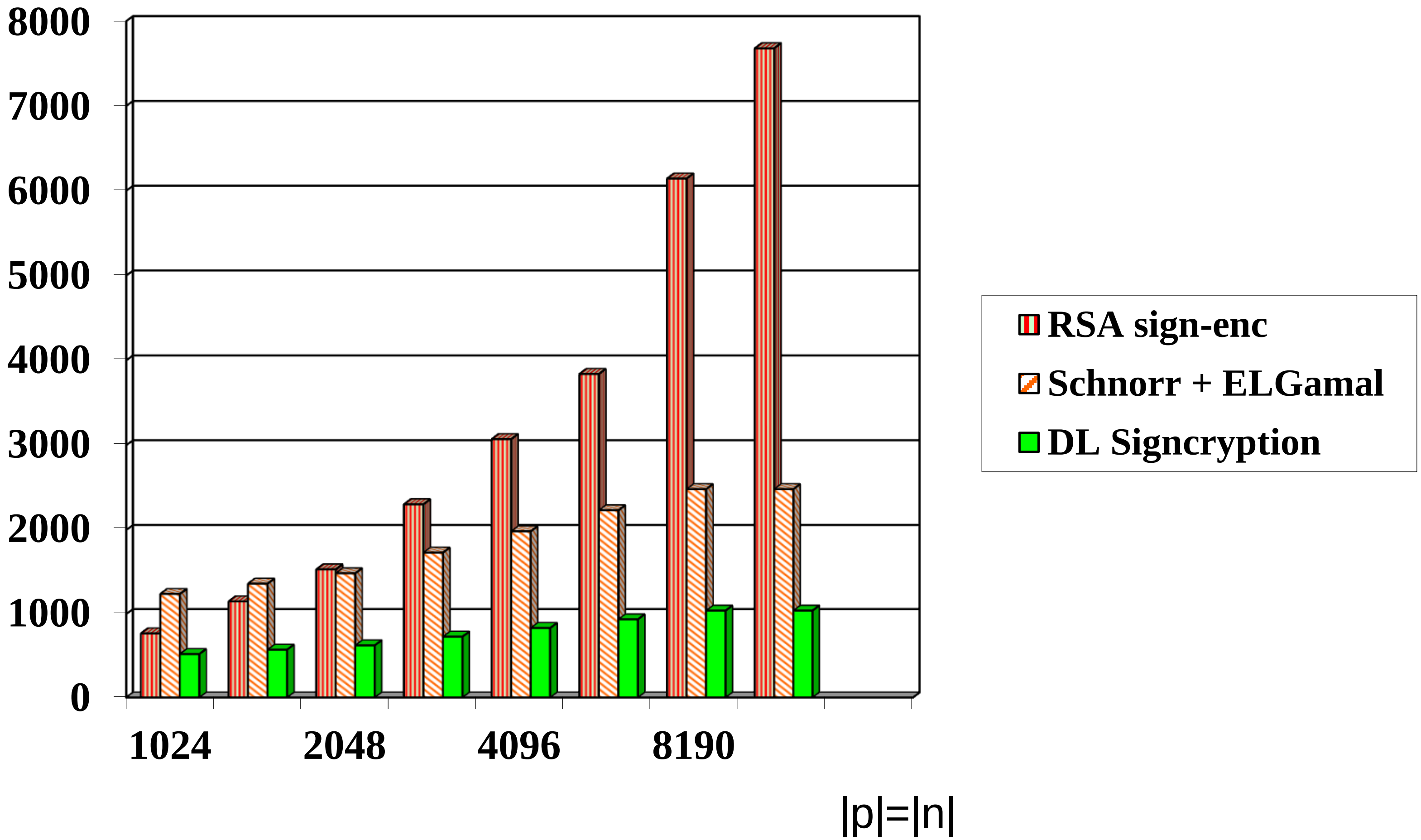
Unsigncryption by Bob:

$(c, r, s) \Longrightarrow m$

- Recover T:
  $T = (y_a \cdot g^r)^{s \cdot x_b} \bmod p$
- $k = G(T, y_a, y_b)$
- $m = D_k(c)$
- $r' = H(T, m, y_a, y_b)$
- if $r' = r$, then accept m; otherwise reject m & indicate ERROR

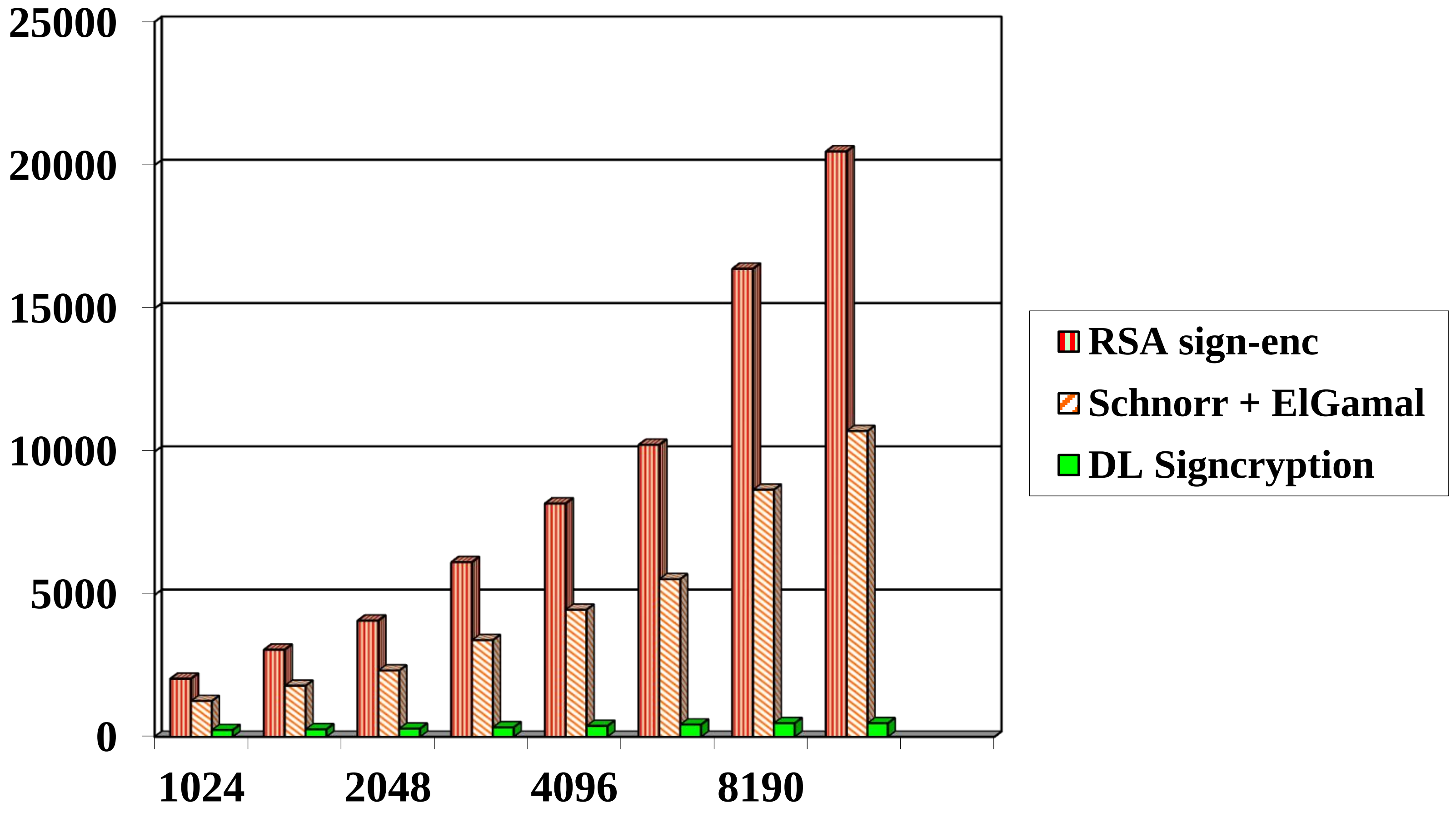
Signcryption: Savings in Computation

Computational Cost (# of multiplications, the smaller the better)

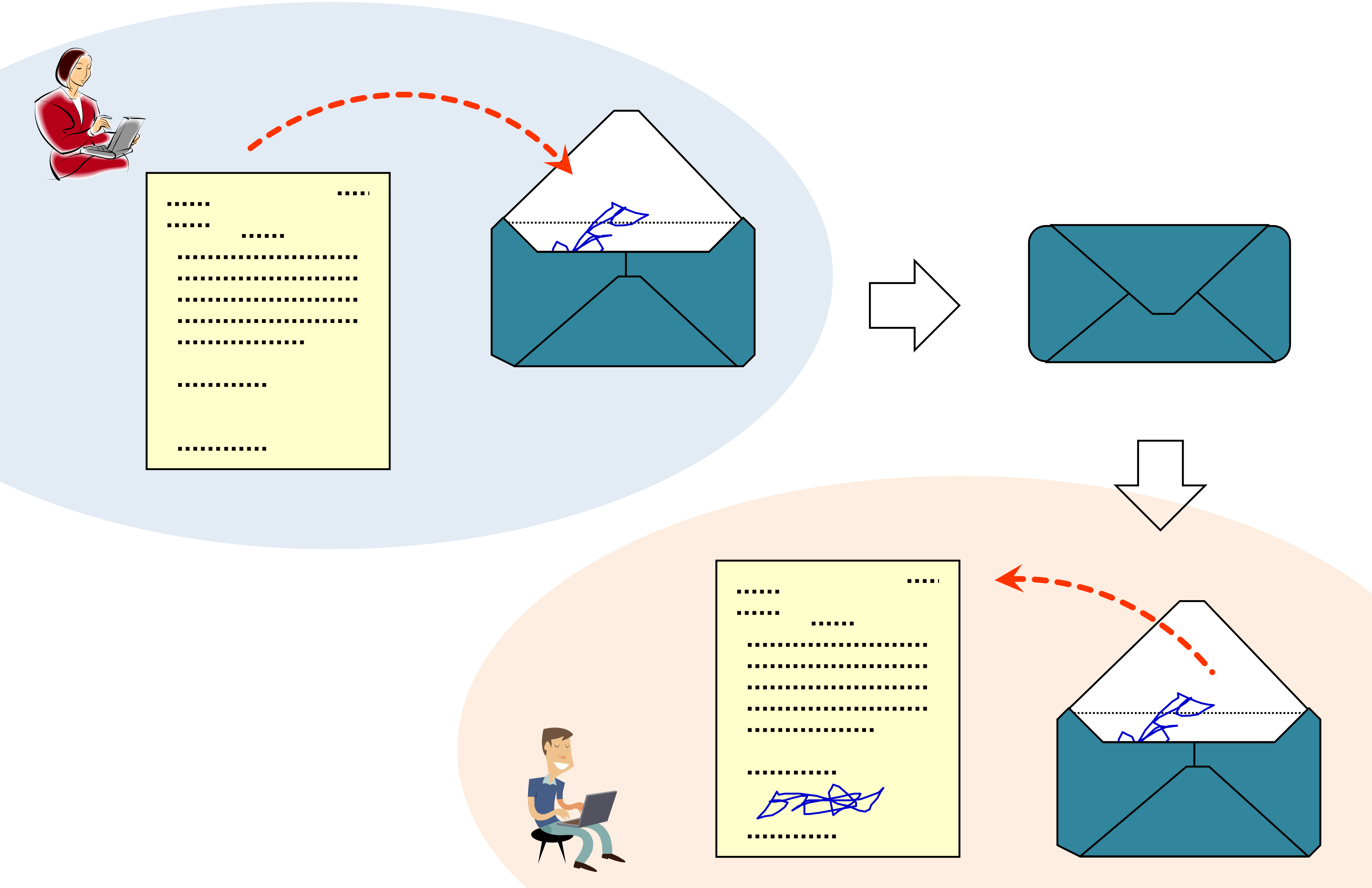


Signcryption: Savings in Communication

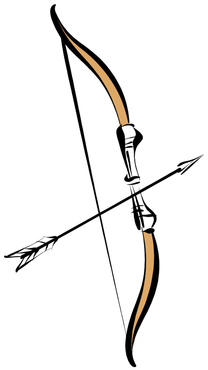
Communication Overhead (# of bits, the smaller the better)



Signcryption as a "Magic" Envelope



The End Result

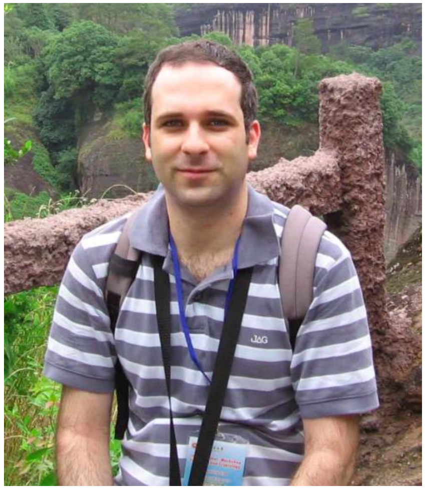


Kill two birds with one stone

Security Model & Proofs

- Security proofs in 2002, with Joonsang Baek & Ron Steinfeld
  - 1st security model
  - 1st mathematical proofs

Joonsang



Ron

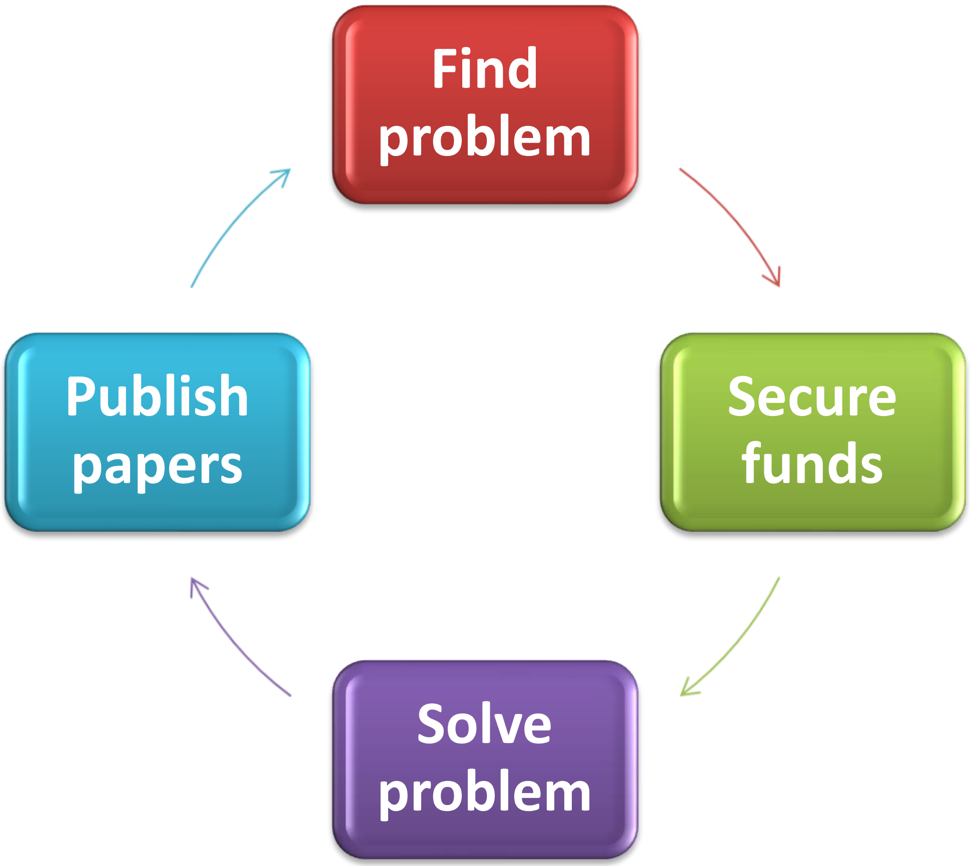
Applications of Signcryption

- Efficient "drop-in" replacement of "signing-then-encrypting"
  - Smartphones & other battery powered devices
- Ad hoc/sensor network security
- Secure SIP for VOIP
- Efficient key establishment
- Many more

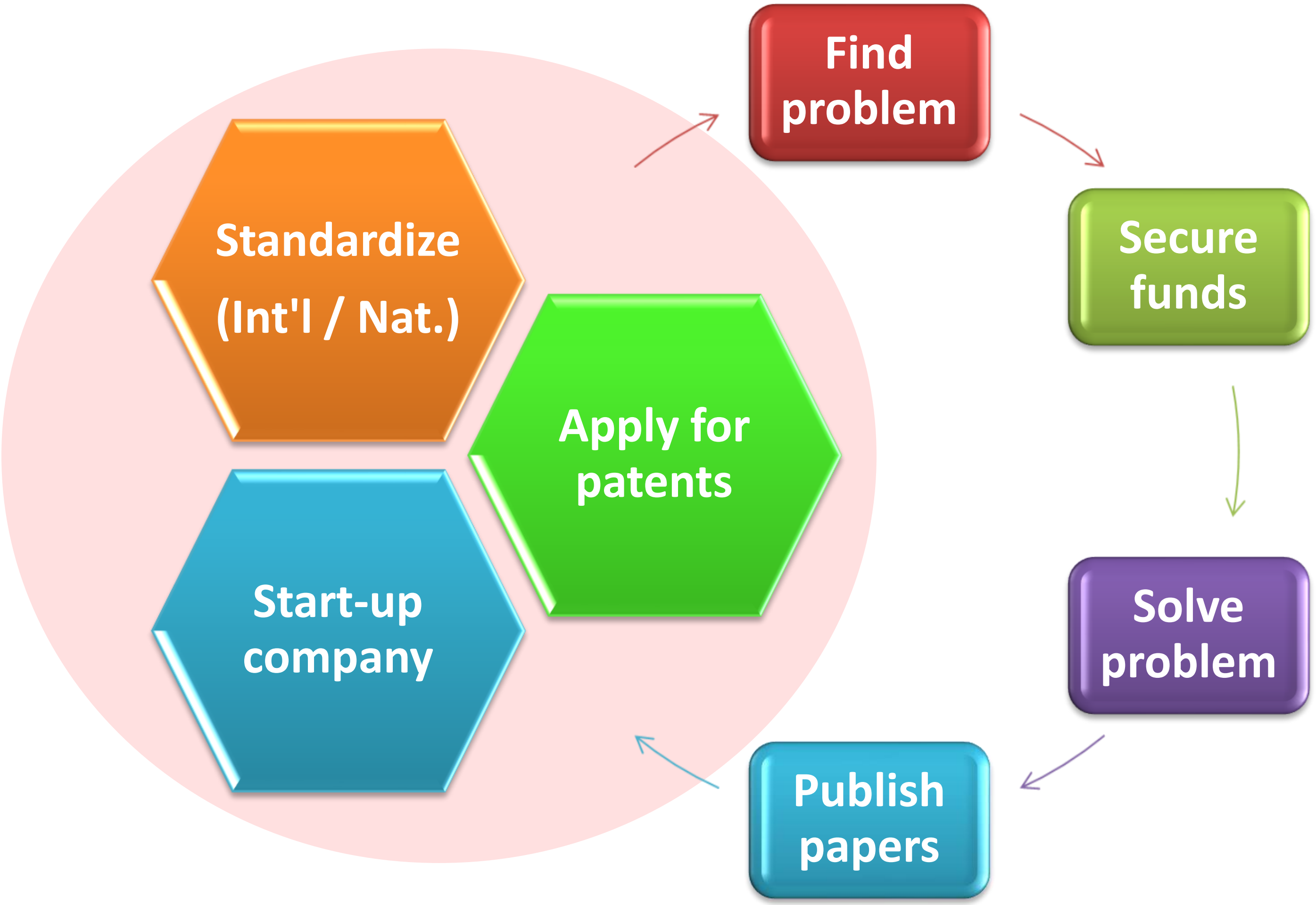
Further Developments

- Extensions: pairing, factorization, ……
- Add "bells and whistles"
  - Multi-recipients, proxy, blind, threshold, ring, ID based, certificateless, ……
- Authenticated encryption (Authencryption)
  - Co-design of shared key authentication and encryption
- New PhD theses

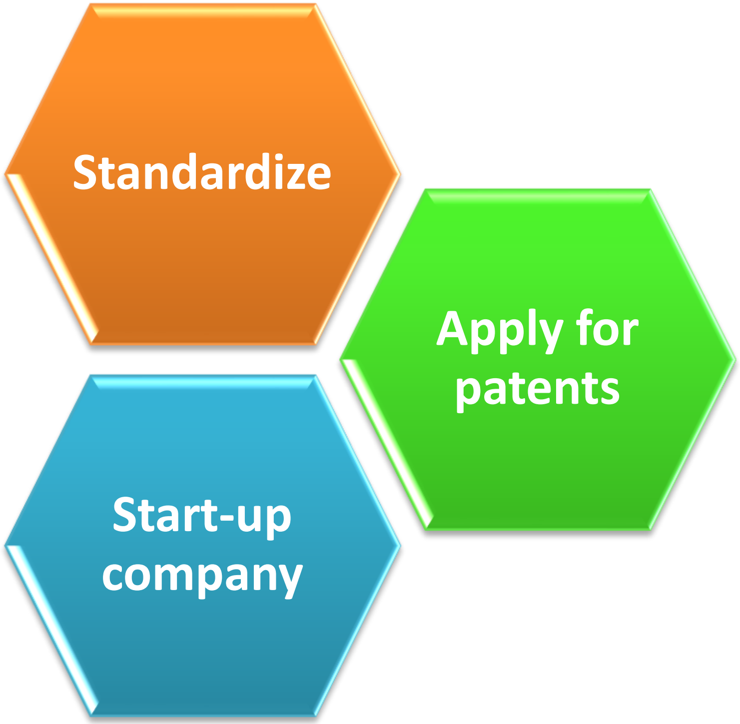
Typical Cycle of Research



Add Commercialization



Commercialization of Signcryption



Signcryption Patents

- **Patents**
  - **Applied in 1996**
  - **Received both in Australia and USA**

- **Support from Prof. Cliff Bellamy**

Transfer of Patent Rights

- **2007**
  - **Sold to** INTELLECTUAL VENTURES® INVESTING IN INVENTION™
- **IV**
  - **Established by ex-Microsoft executive Nathan Myhrvold**
  - **One of the top 5 patent holders in the US**

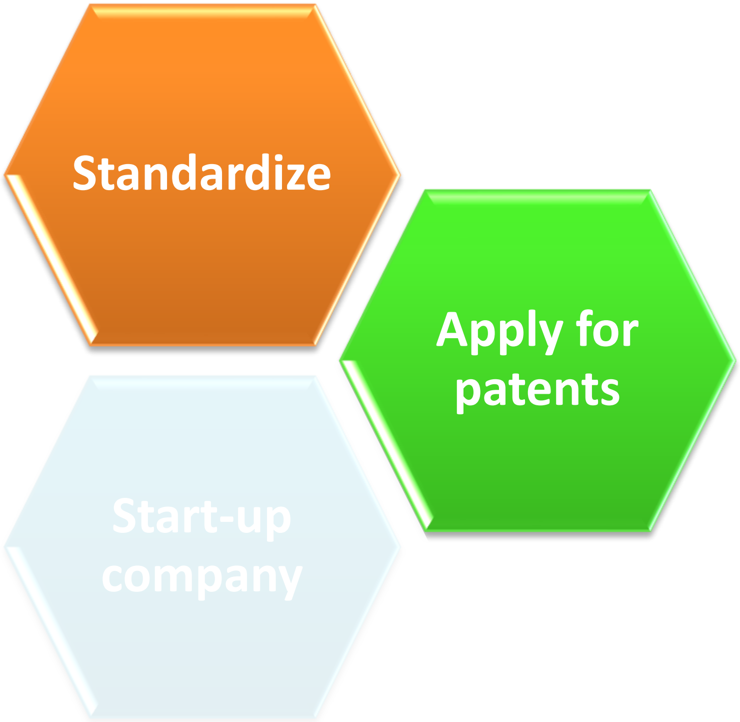
Signcryption Standards

- **In 2006, ISO**

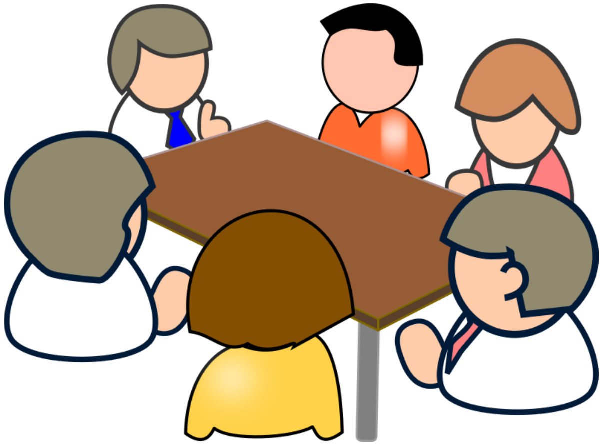
  --- International Standardization Organization ---

  started to look into establishing uniform standard for various signcryption techniques

- **I was notified in 2008**
  - **Accepted invitation to help the standard**



ISO Standardization Process



- ISO/IEC JTC1/SC27,
  "Information technology—
  Security techniques—Signcryption"
- ISO
  - JTC1, SC 27, WG 2
  - 2006, proposal to standardize signcryption
  - Proposal approved in Spring 2008
  - Project #29150 started at ISO Kyoto meeting, April 2008
  - Completed at the end of 2011 (after 4 years work)

ISO Process

- ISO ≈ mini UN
  - 1 country 1 vote
- "textbook" algorithms not adequate
  - Need to be transformed into robust techniques for real-world use
- Face-to-face meetings: twice a year
- Lot of online & offline discussions/telemeetings
- Min. # of stags = 6
- Min. # of years = 4

Personal experience

- Overcoming challenges
  - Time commitments
  - Funding for travelling to meetings
  - Skills to work with delegates from various countries
  - Understanding important non-technical aspects
    - Usability, simplicity, compatibility, acceptability
- Great satisfaction
  - Help industrial experts include best-of-breed crypto techniques into int'l standards
  - Turn "textbook" algorithms into industrial standards
  - Identify problems of practical importance which tend to be ignored in academic research
- Standards bodies embracing expert advice
  - Urge you to consider participation

INTERNATIONAL STANDARD

ISO/IEC 29150

First edition
2011-12-15

Information technology — Security techniques — Signcryption

Technologies de l'information — Techniques de sécurité — Signcryptage

Reference number
ISO/IEC 29150:2011(E)

signcryption.org

- Home
- Introduction
- Standardization
- Publications
- Theses
- Books
- Patents
- Contact

Welcome to Signcryption (ISO 29150)

Signcryption, an international standard for data protection (ISO/IEC 29150), was invented in 1996. Details of the newly discovered public key cryptographic technology were first disclosed to the public at the CRYPTO'97 conference held in Santa Barbara. Since then, I have witnessed a steadily increasing amount of interest in the technology from both researchers and practitioners alike. Each year, extensions, refinements and adaptations of the original techniques are being published at a number of workshops and conferences; advanced degrees are being conferred to graduate students who have chosen signcryption as their research foci; new applications are being developed to take advantage of benefits afforded by signcryption.

To better serve the community of researchers and practitioners who are interested in the technology, I have established this web portal for all information related to signcryption technology. I hope that you find this portal useful.

Your feedback on the web site is important for its accuracy, completeness and relevance. I welcome your comments and suggestions.

Thank you,

Yuliang Zheng
Inventor of Signcryption

What Should/Can be Commercialized

- Practical
- Critical
- Less dependent on other techniques
- Resources available
  - Funds, key persons, time
- Desire to commercialize!
- When not to
  - Too theoretical (no use in 10 years), minor improvement, strong dependency on other patents, no funds
  - We all stand on others' shoulders! --- Not patenting is equally honorable!

http://www.victorialouiserabin.com/

Q & A

Thanks!