Identity Based Encryption
TechTalk

27. Juni 2013
PKI does not solve an important problem:

Alice wants to send a message to Bob. How does she get Bob’s key?
Workaround:

1. Alice gets the key from »somewhere«
2. The key is signed by a CA
3. Alice verifies the signature to ensure it is Bob’s key
4. Alice needs to trust all signing CAs.
You trust these companies.

TÜRKTRUST Elektronik
Chambers of Commerce
Global Chambersign
AddTrust
America Online
AOL Time Warner
Juur-SK
Autoridad de Certificacion Firmaprofesional CIF
Baltimore CyberTrust
Buypass
certSIGN
ePKI
CNNIC
COMODO
ComSign Secured
Cybertrust Global
Deutsche Telekom
DSV-Gruppe
Certigna
DigiCert
DigiNotar
identrust
Disikg
Edicom Group
Bilgi Elektronik
Entrust
Equifax
GeoTrust

GlobalSign
Verizon
Hongkong Post
IPS
JCSINC
Japanese Government
Microsec
NetLock Expressz
Network Solutions
French Government
QuoVadis Global
RSA Security
Security Communication Trust
Trustwave
Certicámara
Sonera
Staat der Nederlanden
Starfield Technologies
StartCom
Swisscom
SwissSign
TrustCenter
TDC Internet
Thawte
Unizeto
VeriSign
Visa
Wells Fargo
XRamp Security
Use the receiver’s identity as a public key (e.g., email address)
The Boneh-Frankling IBE scheme from the Weil Paring:

**Setup** Takes parameter $k$, 
returns *param* and *masterkey*

**Extract** Takes *param*, *masterkey* and $ID \in \{0,1\}^*$, 
returns private key $d$

**Encrypt** Takes *param*, $ID$, and $M \in \mathcal{M}$, 
returns ciphertext $c \in \mathcal{C}$

**Decrypt** Takes *param*, $c \in \mathcal{C}$ and private key $d$, 
returns $M \in \mathcal{M}$

$$\text{Decrypt}(\text{param}, \text{Encrypt}(\text{param}, ID, M), d) = M$$
IBE is one field in *Pairing Based Cryptography*

$\mathbb{G}_1$ and $\mathbb{G}_2$ are groups of order $q$ for a large prime $p$. There is a *bilinear map* $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ with the following properties:

* **Bilinear**
  \[ \hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab} \text{ for all } P, Q \in \mathbb{G}_1 \text{ and all } a, b \in \mathbb{Z} \]

* **Non-degenerate**
  \[ \hat{e}(P, Q) \neq 1 \]

* **Computable**
  It can be efficiently computed
How such a pairing is created is a different field. Just accept it's there.

Known pairings: *Weil, Tate, Ate, Twisted Ate, η*  
→ Groups and mappings over hyperelliptic curves
Pairing-Based Crypto is special:

Computational Diffie-Hellman Assumption → Bilinear Diffie-Hellman Assumption
IND-CCA → IND-ID-CCA
IND-CPA → IND-ID-CPA
Advantages of IBE (and IBS)

- No PKI required (!)
- No a priori key exchange required (!)
- User does not need to manage her private key
- Signatures which only the legitimate receiver can verify
Disadvantages of IBE

- KG can create private key for any ID
  (»key escrow«, ← can even be a desired property)
- Key revocation is not easy
- Foundations are different from »mature« crypto
Can I use IBE?

Yes.

- Stanford IBE System
  (Boneh et al.)

- MIRACL
  (with compiler for embedded system processors)

- Voltage Security
  (commercial, w. plugin for MS Outlook)
thx.