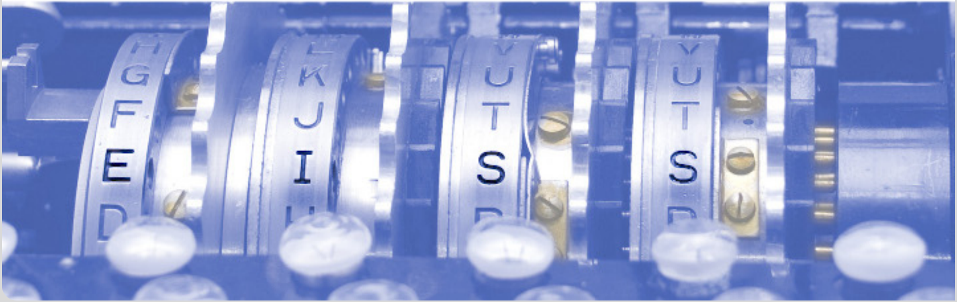
Karlsruhe Institute of Technology

Cryptographic Building Blocks

CS 858

Christian Henrich | October 5, 2010

INSTITUTE OF CRYPTOGRAPHY AND SECURITY



Textbook RSA

Karlsruhe Institute of Technology

KeyGen
1. choose $p, q \xleftarrow{R} \mathbb{P}$
2. set $n := p \cdot q$
3. find e, d with $e \cdot d \equiv 1 \mod \varphi(n)$
4. $pk = (e, n)$, $sk = d$

$\textsc{Enc}(pk, m)$ $c \equiv m^e \mod n$

$\textsc{Dec}(sk, c)$ $m \equiv c^d \mod n$

Homorphic Property

Homorphic Property

$$
\begin{aligned}
\textsc{Enc}(pk, m_1) \cdot \textsc{Enc}(pk, m_2) &\equiv m_1^e \cdot m_2^e \\
&\equiv (m_1 \cdot m_2)^e \\
&\equiv \textsc{Enc}(pk, m_1 \cdot m_2)
\end{aligned}
$$

Problem: Textbook RSA is deterministic.

ElGamal

KeyGen

1. multiplicative group $(G, \cdot)$ with generator g
2. choose $x \xleftarrow{R} \{1, \ldots, |G|\}$
3. set $y := g^x$
4. $pk = y$, $sk = x$

Enc(pk, m) $r \xleftarrow{R} \{1, \ldots, |G|\}$, $(c_1, c_2) = (g^r, y^r \cdot m)$

Dec$(sk, (c_1, c_2))$ $m = c_2 \cdot (c_1^x)^{-1}$

Homorphic Properties

$$\begin{aligned}
\textsc{Enc}(pk, m_1) \cdot \textsc{Enc}(pk, m_2) &= (g^{r_1}, y^{r_1} \cdot m_1) \cdot (g^{r_2}, y^{r_2} \cdot m_2) \\
&\equiv (g^{r_1+r_2}, y^{r_1+r_2} \cdot m_1 \cdot m_2) \\
&\equiv \textsc{Enc}(pk, m_1 \cdot m_2) \\
(1, n) \cdot \textsc{Enc}(pk, m) &= (g^r, n \cdot y^r \cdot m) \\
&\equiv \textsc{Enc}(pk, n \cdot m)
\end{aligned}$$

Problem: ElGamal is not deterministic, but malleable.

RSA Signatures

KeyGen
1. choose $p, q \xleftarrow{R} \mathbb{P}$
2. set $n := p \cdot q$
3. find e, d with $e \cdot d \equiv 1 \mod \varphi(n)$
4. $sk = e, vk = (d, n)$

$\textsc{Sign}(sk, m)$ $s \equiv m^e \mod n$

$\textsc{Verify}(vk, m, s)$ $m \overset{?}{\equiv} c^d \mod n$

Blind Signatures

Karlsruhe Institute of Technology

1. Alice chooses masking c and sends $\widetilde{m} = c^d \cdot m$ to Bob.
2. Bob signs $\widetilde{m}$ and sends signature $\widetilde{s} = \widetilde{m}^e$ to Alice.
3. Alice removes masking from $\widetilde{s} = \widetilde{m}^e = c^{ed} \cdot m^e$ and obtains $s = \widetilde{s} \cdot c^{-1} = m^e$ as a signature for m.

Commitment Schemes

COMMIT Commit to a value *m*.

OPEN Open a commitment *c* to a value *m*.

Commitment Scheme from Hash Function

Karlsruhe Institute of Technology

SETUP	Choose keyed hash function $h(\cdot,\cdot)$.
COMMIT	Commit to m by choosing randomness r and sending $c = h(r, m)$.
OPEN	Send preimages r, m to commitment c.

Properties

binding	from collision resistance
hiding	from one-way property

Pedersen Commitments

SETUP	Choose multiplicative group $(G, \cdot)$ with generators g, h.
COMMIT	Commit to m by by choosing randomness r and sending $c = g^r \cdot h^m$.
OPEN	Send m and r.

Properties

binding	*dlog-assumption:* $\log_g h$ is hard to compute
hiding	unconditionally binding

Selective Credentials

The signed credential contains commitments to values. The issuer signs the credential blind.

Name	COMMIT(Christian Henrich)
Address	COMMIT(...)
Age	COMMIT(...)
Date of Birth	COMMIT(...)
	$s = \textsc{Sign}(sk, \text{credential})$

J. Holt, K. Seamus: *Selective Disclosure Credential Sets*

Zero Knowledge Proofs

Karlsruhe Institute of Technology

Proofer Peggy knows an isomorphism Φ between two graphs G_0 and G_1 and wants to prove this to verifier Victor.

Protocol

1. Peggy chooses isomorphism $\Psi \xleftarrow{R}$ and sends $G' = \Psi(G_0)$ to Victor.
2. Victor chooses challenge bit $b \xleftarrow{R} \{0, 1\}$.
3. $b = 0$ Peggy sends Ψ to Victor.
   $b = 1$ Peggy sends $\Psi \circ \Phi$ to Victor.

After k runs Victor is convinced Peggy knows Φ without getting any more information.