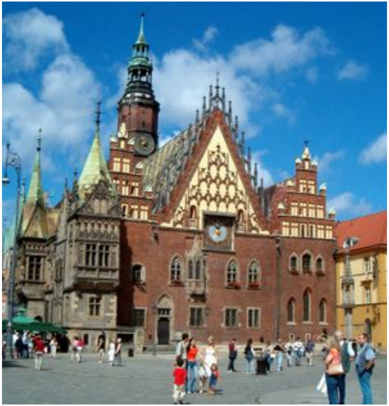
Practical Deniable Encryption

Marek Klonowski, Przemysław Kubiak,
Mirosław Kutyłowski

Wrocław University of Technology

Nový Smokovec, January 2008

Wrocław



Motivation

- We believe that the adversary cannot decrypt the ciphertext without the private key, but ...

Motivation

- We believe that the adversary cannot decrypt the ciphertext without the private key, but ...
- strong adversary has a power to demand a private key (violence, law enforcement procedures).

Coercion in regular encryption scheme

Regular encryption

- Encryption:

$$m - \text{message}$$
$$c = Enc(m, r)$$

- Decryption:

$$m = Dec(c)$$

Coercion in regular encryption scheme

In case of coercion one can ...

- refuse presenting the key (key is lost or forgotten)
- reveal a fake parameters r' instead r, such that $Enc(m, r) = Enc(m_f, r')$ and m_f is “legal”.

Idea of the solution due to Canetti et al.

"Deniable Encryption" due to R.Canetti,C.Dwork,M.Naor,R.Ostovski[CRYPTO 97]

(Sender) deniable encryption:

$\phi(\cdot,\cdot,\cdot,\cdot)$ – faking algorithm

$r' := \phi(m, m_f, c, r)$ such that $c = Enc(m_f, r')$

Idea of the solution due to Canetti et al.

“Deniable Encryption” due to R.Canetti,C.Dwork,M.Naor,R.Ostovski[CRYPTO 97]

(Sender) deniable encryption:

$$\phi(\cdot,\cdot,\cdot,\cdot) \text{ -- faking algorithm}$$

$$r' := \phi(m, m_f, c, r) \text{ such that } c = Enc(m_f, r')$$

In case of coercion, (sender,reciver) reveals “legal” m_f and r' instead of “banned” m and r.

Scheme of Canetti al.

Translucent set

Family $\mathcal{S}_t$ is called *translucent set* if

- $\mathcal{S}_t \subset \{0,1\}^t$ and $|\mathcal{S}_t| < 2^{t-k}$, for sufficiently large $k(t)$.
- It is easy to find random element $x \in \mathcal{S}_t$
- Given $x \in \{0,1\}^t$ and trapdoor information d it is easy to check if $x \in \mathcal{S}_t$
- Without d it is not computationally feasible to decide if $x \in \mathcal{S}_t$

Translucent set: construction

f- one way permutation, B – hard core-predicate

$$\mathcal{S}_t = \{x = x_0||b_1||\ldots||b_k \in \{0,1\}^{s+k} | (\forall_{i \le k}) B(f^{-i}(x_0) = b_i)\}$$

Scheme of Canetti al.

Encryption

Encryption:

- $S \in S_t$, R – randomly chosen from $\{0,1\}^t$
- To encrypt 0 (resp. 1) odd (resp. even) number $i \in 1 \ldots n$ is chosen.
- Ciphrertext of single bit consist of i S-elements followed by $n - i$ R-elements.

Decryption: Parity of S-elements points if the ciphertext encodes 1 or 0.

Scheme of Canetti al.

Opening single bit

Honest Opening: The Sender reveals the real random choices used during encoding.

Dishonest Opening: Parity is changed - single S-element is claimed to be randomly chosen R.

Scheme of Canetti al.

Opening single bit

Honest Opening: The Sender reveals the real random choices used during encoding.

Dishonest Opening: Parity is changed - single S-element is claimed to be randomly chosen R.

- Scheme provides sender-deniability
- More effective modifications of the basic scheme were presented

Nested construction based on Canetti et al.'s protocol

Motivation

- Coercer knows that the deniable encryption scheme is used. So the coercer can demand the "true" message.
- Idea: to reveal faked m_f, on the second demand reveal also "slightly banned" m'_f, but the real message m is hidden in a deeper layer.

Nested construction

Nested translucent sets

Let $t = s + 2k$. Represent each $x \in \{0,1\}^{t+2k}$ as

$$x = x_0 || b_1^\star || \ldots || b_k^\star || b_1 || \ldots || b_k,$$

where $x_0 \in \{0,1\}^s$ is followed by $2k$ bits. Then we define translucent sets as:

$$\mathcal{S}_t^\star = \{x = x_0 || b_1^\star || \ldots || b_k^\star || b_1 || \ldots || b_k | (\forall_i \le k) B(f^{\star -1}(x_0) = b_i^\star\}$$

and

$$\mathcal{S}_t = \{x_0 || b_1^\star \ldots || b_k^\star || b_1 || \ldots || b_k | (\forall_i \le k) B(f^{-1}(x_0 || b_1^\star \ldots || b_k^\star) = b_i\}$$

Nested construction

Russian dolls - like encryption

- at the price of bandwith of the information channel we can embedded more than two layers of deniability,
- hierarchy of “banned” messages- coercer does not know where the bottom is.

Postponed One-Time Pad

Outline

- shared key, provides sender (sender-and-receiver) deniability
- very efficient (size of the ciphertext, computational complexity)
- on principle,can be built on the top of any encryption scheme
- allows to deny *d* consecutive encrypted message

Postponed One-Time Pad, basic version

Preliminaries

Global parameters:

- $\mathfrak{R} = \mathbb{F}_{2^{128}}$
- $E : \mathfrak{R} \to \mathfrak{R}$, encryption scheme
- $a_1, a_2, F(a_1)$ global parameters from $\mathfrak{R}$

Secret information shared by the sender and the receiver:

- $R : \mathfrak{R} \to \mathfrak{R}$, random polynomial
- $b \in \mathfrak{R}$

Postponed One-Time Pad, basic version

Encryption

In order to send message m_i sender computes:

1. $E(m_i)$ - regular ciphertext of m_i,
2. $b := R(b)$,
3. F_i – straight line determined by $(a_1, F(a_1)), (b, E(m))$,
4. the ciphertext $F_i(a_2)$ is sent to the receiver.

Postponed One-Time Pad, basic version

Encryption

In order to send message m_i sender computes:

1. $E(m_i)$ - regular ciphertext of m_i,
2. $b := R(b)$,
3. F_i – straight line determined by $(a_1, F(a_1))$, $(b, E(m))$,
4. the ciphertext $F_i(a_2)$ is sent to the receiver.

Decryption

Since the receiver can get actual value of b, he can find $F_i(b)$ and then $m_i = E^{-1}(F(b))$

Postponed One-Time Pad, basic version

Dishonest opening -idea

For any set d of messages $m_{f,1}, m_{f,2}, \ldots, m_{f,d}$ it is easy to reconstruct a polynomial R_f such that gives results that are coherent with previously sent values and decryption procedure gives $m_{f,1}, m_{f,2}, \ldots, m_{f,d}$.

Postponed One-Time Pad, basic version

Dishonest opening -idea

For any set d of messages $m_{f,1}, m_{f,2}, \ldots, m_{f,d}$ it is easy to reconstruct a polynomial R_f such that gives results that are coherent with previously sent values and decryption procedure gives $m_{f,1}, m_{f,2}, \ldots, m_{f,d}$.

Details of this scheme are described in the paper

ElGamal -based deniable encryption

Idea

- Scheme perfectly mimics regular ElGamal encryption scheme.
- Sender and receiver share a secret key of regular ElGamal scheme.
- Fake message m_f must be fixed in advance.
- Board band subliminal channel

ElGamal -based deniable encryption

Idea

- Scheme perfectly mimics regular ElGamal encryption scheme.
- Sender and receiver share a secret key of regular ElGamal scheme.
- Fake message m_f must be fixed in advance.
- Board band subliminal channel

Preliminaries

- Public parameters – $0 < x < p - 1$ is a private key, public key is $y = g^x$.
- Sender and receiver share a secret s and the receiver reveals his secret key x to the sender.

ElGamal -based deniable encryption

Encryption

- $k = HASH(s||m_f)$ is computed
- $$\begin{aligned} \alpha &:= g^k \cdot m, \\ \beta &:= (y^k \cdot m^x) \cdot m_f. \end{aligned}$$

ElGamal -based deniable encryption

Decryption

Having s and x one can easily retrieve m

$$\frac{\beta}{\alpha^x} = \frac{y^k \cdot m^x \cdot m_f}{g^{kx} \cdot m^x} = m_f \ .$$

$$k := HASH(s||m_f)$$

$$m := \beta(g)^{-k}$$

Faked decryption

Receiver can reveal x. The attacker can check that this message is in fact a regular, valid ElGamal encryption of the message m_f

Some other ideas

- subliminal channel in other schemes
- embedding covert channel in deniable encryption schems

THANK YOU FOR YOUR ATTENTION