Parallel Signcryption

Josef Pieprzyk
(joint work with Tarun Bansal and Xavier Boyen)

Data61, CSIRO &
Computer Science Institute
PAN, Warsaw, Poland

June 2019

Road Map

Introduction

- Zheng 1997 – concept of signcryption
  cost(signcrypt) $<$ cost(sign)$+$cost(encrypt)
- An, Dodis, Rabin 2002 – three generic schemes
  - $*$ encrypt-then-sign (EtS)
  - $*$ sign-then-encrypt (StE)
  - $*$ commit-then-sign-and-encrypt (CtS&E), n.b. sign-and-encrypt" (S&E) may reveal information about messages
- Pieprzyk, Pointcheval 2003 – share-then-sign-and-encrypt (parallel signcryption)

Security Models

- Outsider security – adversary knows public keys for signing and encryption
- Insider security – adversary is one of the parties either
  - sender who wants to compromise the receiver secret key or
  - receiver who wants to compromise the sender secret key
- multiuser security – adversary can interact with many users and compromise some of them (we need a unique identity for each user)

Limitations of Existing Solutions

- Majority of signcryptions are StE or EtS including sequential KEM/DEM hybrids – limited speed
- CtS&E permits for parallel signing and encrypting but accepts relatively short messages
- Many schemes are built using very specific intractability assumptions (Factoring, DL, DH, etc.)
- There is no hybrid signcryption that is IND-CCA/UF and built from weaker security assumptions on signature and encryption algorithms

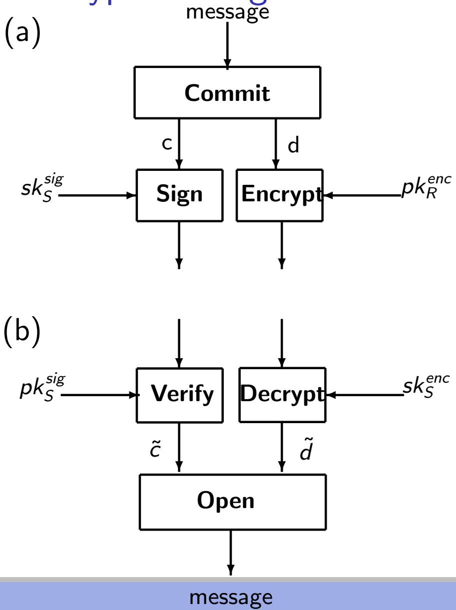
CtS&E-type Signcryption

Schemes	Model	Encryption	Signature	Message Length	# of other Functions	Signcryption
An et al.[1]	No Specific	IND-CCA	UF-CMA	Restricted	Commitment scheme	IND-gCCA/UF-CMA
Pieprzyk et al. [5]	Random Oracle	OW-CPA	suUF-RMA	Restricted	3 hash, 1 Secret share scheme	IND-CCA/sUF-CMA
Dodis et al. [4][3]	Random Oracle	OW-CPA	sUF-CMA	Restricted	1 Hash, 1 Commitment scheme	IND-CCA/sUF-CMA
				Unrestricted	1 Hash, 1 Commitment scheme, Symmetric encryption	
Our Result	Ideal Permutation	OW-CPA	suUF-RMA	Unrestricted	1 SpongeWrap, 1 Sponge Function (≊2 Hash)	IND-CCA/sUF-CMA
		OW-PCA	uUF-RMA			IND-CCA/UF-CMA

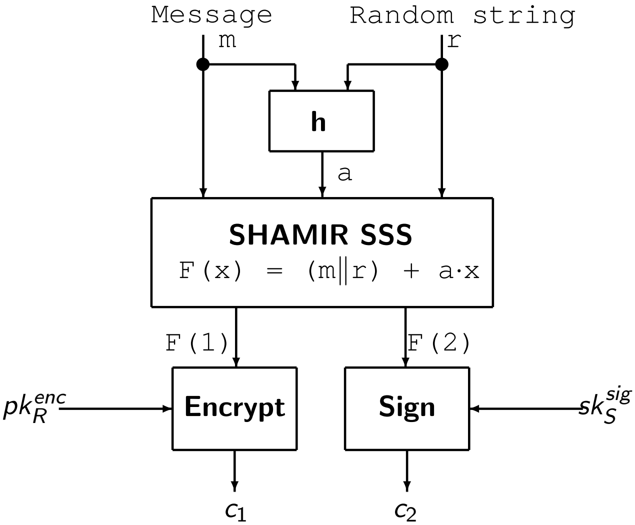
Note that IND stands for indistinguishability, OW for one-wayness, CPA/CMA for chosen plaintext/message attack, CCA for chosen ciphertext-attack, UF for existential unforgeability, uUF for universal unforgeability, suUF for strong uUF, RMA for random message attack, gCCA for generic-CCA, OW-CPA for trapdoor one-way permutation and OW-PCA for one-wayness under plaintext-checking attack.

Road Map

Commit-then-Encrypt-and-Sign



Generic Share-then-Encrypt-and-Sign



Security of Generic Share-then-Encrypt-and-Sign

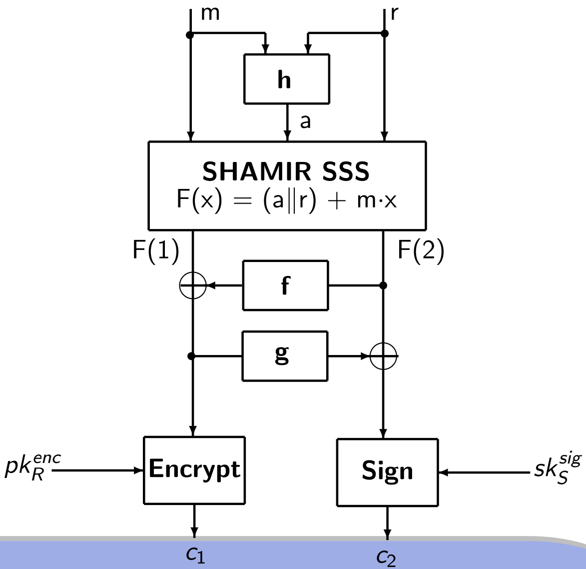
Theorem

If

- *encryption is IND-CCA and*
- *signature is deterministic UF-RMA*

then parallel signcryption scheme, on message $ID_S||m$ *is IND-CCA and UF-CMA secure in the insider-security model for the multi-user setting.*

Optimal Parallel Signcryption



Security of Optimal Parallel Signcryption

Theorem

If

- *encryption is deterministic and OW-CPA secure, and*
- *signature is deterministic and uUF-RMA secure*

then the optimal parallel signcryption is multi-user insider FSO/FUO-IND-CCA and multi-user insider FSO/FUO-UF-CMA secure,

FSO/FUO-IND-CCA stands for *indistinguishability of signcryptext against chosen ciphertext attack with access to 'flexible' signcryption/unsigncryption oracles* and
FSO/FUO-UF-CMA – *unforgeability under chosen message attack with access to 'flexible' signcryption/unsigncryption oracles*

Road Map

Contributions

- Two signcryptions in ideal-permutation model with sponge structure:
  - ∗ parallel signcryption for a fixed message length
  - ∗ parallel signcryption for messages of arbitrary length
- Signcryptions achieve the IND-CCA/UF-CMA security under weak security assumptions on signature and encryption (security amplification)
- We need three building blocks: encryption, signature and ideal permutation (sponge)
- Due to sponge, signcryptions scale well for messages of arbitrary lengths

Building Blocks

- Ideal permutation
$$\pi : D \longrightarrow R$$
where $D = R = \{0,1\}^b$ and π is chosen uniformly at random from all permutations on D
- Public-key encryption with
  - $\mathrm{GenEnc}(1^k)$ that produces a pair $(\mathrm{pk}, \mathrm{sk})$, where k is a security parameter
  - $\mathrm{Enc}_{\mathrm{pk}}(m; g) = c$ that outputs a ciphertext c for a message $m \in \mathcal{M}$ and a public key pk using random coins $g \in \mathtt{COINS}$.
  - $\mathrm{Dec}_{sk}(c)$ that recovers a message m from a ciphertext c using sk
- Signature with
  - $\mathrm{GenSign}(1^k)$ outputs a pair (pk,sk)
  - $\mathrm{Sign}_{\mathrm{sk}}(M)$ outputs a signature σ
  - $\mathrm{Ver}_{\mathrm{pk}}(\sigma, M)$ generates either valid $\top$ or invalid $\perp$

Security Notions - Encryption

- OW – one-wayness – knowing c and public key pk, it is difficult to find m
- OW-PCA – one-wayness when adversary $\mathcal{A}$ has access to plaintext checking oracle ($\mathcal{O}^{PC}$)
- IND – indistinguishability of encryptions

$$\mathsf{Adv}^{\mathsf{ind}}_{\mathrm{ENCRYPT}}(\mathcal{A}) = 2\times\Pr\left[\begin{array}{l}(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{GenEnc}(1^k), (m_0, m_1, s) \leftarrow \mathcal{A}_1(\mathsf{pk}),\\ b \in \{0,1\}, c = \mathsf{Enc}_{\mathsf{pk}}(m_b) : \mathcal{A}_2(m_0, m_1, s, c) = b\end{array}\right] - 1$$

Attacks - Encryption

- CPA – chosen-plaintext attack – adversary has access to the encryption oracle
- CCA – chosen-ciphertext attack – adversary has access to both enc/dec oracles (with exception for the target ciphertext)

Security Notions – Signature

The adversary knows pk and queries signature oracle.

- Existential unforgeability (UF) – $\mathcal{A}$ wins if it outputs a pair (m^*, σ^*), where $\mathsf{Ver}_{\mathsf{pk}}(m^*, \sigma^*) = \top$ and $\mathcal{A}$ never queried the signature oracle with m^*.
- Strong existential unforgeability (sUF) – UF + $\mathcal{A}$ never received the response σ^* while interacting with the signature oracle
- Universal unforgeability (uUF) – UF + m^* is randomly chosen
- Strong universally unforgeability (suUF) – uUF + $\mathcal{A}$ never received the response σ^* while interacting with the signature oracle

Signcryption – Definition

A triplet of the following algorithms:

- Gen – for a security parameter k, outputs keys (SDK,VEK), where
  - SDK is the secret user's sign/decrypt key and
  - VEK is the public user's verify/encrypt key
- SignEnc – the encryption and signing algorithm which produces

$$Y = \mathrm{SignEnc}_{\mathrm{SDK}_S,\mathrm{VEK}_R}(M)$$

  for a message M, the public key of the receiver VEK_R and private key of sender SDK_S
- VerDec – the decryption and verifying algorithm which recovers the message

$$M = \mathrm{VerDec}_{\mathrm{SDK}_R,\mathrm{VEK}_S}(Y)$$

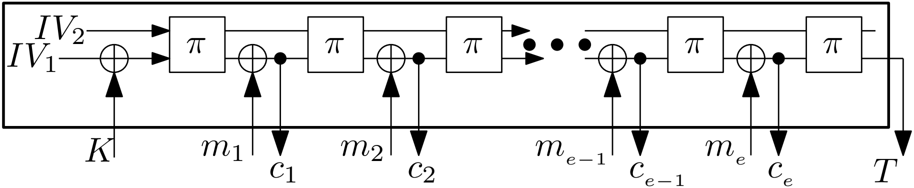
  if M is valid. Otherwise, it returns $\perp$

Signcryption - Security Notions

- Existential forgery (UF) – $\mathcal{A}$ produces a valid signed ciphertext for a new message
- Indistinguishability (IND) – $\mathcal{A}$ is able to assign a challenge ciphertext to one of two messages of their choice with non-negligible probability

Road Map

SpWrap – Sponge-based Padding



SpWrap - Encryption and Decryption

$\underline{SpWrap.Enc(K, M, IV_1||IV_2, r, k, \ell_{sg})}$

1 $x = IV_1$; $w = IV_2$;

2 checkin(M, r, k, ℓ_{sg})=$m_1|| \ldots ||m_{(n+1)}$

3 $x = IV_1 \oplus 0^{(r-k)}||K$

4 **for** $i = 1 \rightarrow n+1$ **do**
  - $(x||w) = \pi(x||w)$
  - $x = x \oplus m_i$
  - $c_i = x$

5 $(x||w) = \pi(x||w)$; $T = \lfloor x \rfloor_k$

6 Return: $C||T = c_1||c_2|| \ldots ||c_{n+1}||T$

$\underline{SpWrap.Dec(K, C||T, IV_1||IV_2, r, k, \ell_{sg})}$

1 $c_1||c_2|| \ldots ||c_{n+1}||T = C||T$ where each $| c_i | = r$

2 $x = IV_1 \oplus 0^{(r-k)}||K$; $w = IV_2$

3 **for** $i = 1 \rightarrow n+1$ **do**
  - $(x||w) = \pi(x||w)$
  - $m_i = x \oplus c_i$
  - $x = c_i$

4 $(x||w) = \pi(x||w)$; $T' = \lfloor x \rfloor_k$

5 $X' = m_1|| \ldots ||m_{n+1}$;

6 **if** $T == T'$ **then**
  - **If** $\exists$ M s.t. M =checkout(X', r, k, ℓ_{sg}) **then** Return:M **else** Return: $\perp$

else
  - $\perp$

SpWrap - checkin and checkout

checkin(M, r, k, ℓ_{sg})

1. $X_1 || X_2 = pad(M, r)$, where $| X_2 | = \ell_{sg} - r$
2. $X_1 || 0^r || X_2 = m_1 || m_2 || \ldots || m_{n+1}$, where $|m_i| = r \; \forall 1 \leq i \leq (n+1)$ and $\exists \; m_i = 0^r$ such that $m_1 || \ldots m_{i-1} = X_1$
3. return: $m_1 || m_2 || \ldots || m_{n+1}$

checkout(X, r, k, ℓ_{sg})

1. **if** $\exists X_1, X_2 \; s.t. \; X_1 || 0^r || X_2 == X$, *where* $| X_2 | = \ell_{sg} - r$ **then**
   $X' = X_1 || X_2$
   else
   Return $\perp$
2. Return: $unpad(X', r)$

$pad(x, r)$

$X = x||1||0^{r-(|x|+1 \bmod r)-1}||1$

return X.

$unpad(y, r)$

{

if $\exists \; x \neq empty \; s.t. \; x||1||0^z||1 = y$ *where* $0 \leq z \leq r - 1$ **then**

return x

else

return $\perp$

}

Sponge

$\underline{Sponge(IV_1||IV_3, J)}$

1 $x||w = IV_1||IV_3$ where $|x| = r$

2 $j_1||j_2||\ldots||j_n = pad(J, r)$, where $|j_i| = r\ \forall 1 \leq i \leq n$.

3 **for** $i = 1 \rightarrow n$ **do**

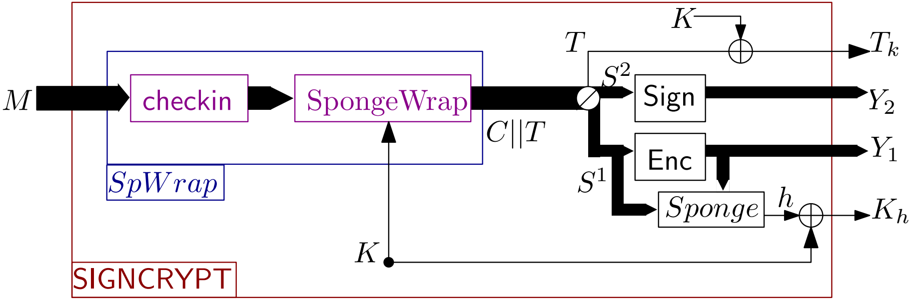
  $x = x \oplus j_i$

  $x||w = \pi(x||w)$

4 Return $\lfloor x \rfloor_k$

Road Map

Parallel Signcryption: SIGNCRYPT



SIGNCRYPT

$\mathsf{SignEnc}_{\mathsf{sk}_S,\mathsf{pk}_R}(M)$

- Initialization: $x = IV_1 = 0^r$, $w = IV_2 = 0^c$, $IV_3 = IV_2 \oplus 1$,
- Random Key: $K \xleftarrow{\$} \{0,1\}^k$;
- checkin(M, r, k, ℓ)=$m_1||\dots||m_{(n+1)}$
- $x = ID_S||ID_R||K$
- **for** $i = 1 \to n+1$ **do**
  - $(x||w) = \pi(x||w)$
  - $x = x \oplus m_i$
  - $c_i = x$
- $(x||w) = \pi(x||w)$; $T = \lfloor x \rfloor_k$
- $(S^1)||(S^2) = (c_1||\dots||c_e)||(c_{e+1}||\dots||c_{n+1})$
- $Y_1 = \mathsf{Enc}_{\mathsf{pk}_R}(S^1)$, $\sigma = \mathsf{Sign}_{\mathsf{sk}_S}(S^2)$
- $pad(S^1||Y_1)$=$y_1||\dots||y_j$; $x = IV_1$; $w = IV_3$
- **for** $i = 1 \to j$ **do**
  - $(x||w) = \pi((x \oplus y_i)||w)$
- $K_h = \lfloor x \rfloor_k \oplus K$; $T_k = T \oplus K$
- Return: $(K_h, Y_1, Y_2 = (S^2, \sigma), T_k)$

$\mathsf{VerDec}_{\mathsf{sk}_R,\mathsf{pk}_S}(K_h, Y_1, Y_2, T_k)$

- Initialization: $IV_1 = 0^r$, $IV_2 = 0^c$, $IV_3 = IV_2 \oplus 1$,
- $S^1 = \mathsf{Dec}_{\mathsf{sk}_R}(Y_1)$; $x = IV_1$, $w = IV_3$;
- **if** $Ver_{pk_S}(Y_2 = (S^2, \sigma)) == \perp$ **then**
  - Return $\perp$
- $(c_1||\dots||c_e)||(c_{e+1}||\dots||c_{n+1}) = (S^1)||(S^2)$
- $pad(S^1||Y_1)$=$y_1||\dots||y_j$;
- **for** $i = 1 \to j$ **do**
  - $(x||w) = \pi((x \oplus y_i)||w)$
- $K = \lfloor x \rfloor_k \oplus K_h$; $T = T_k \oplus K$
- $x = ID_S||ID_R||K$; $w = IV_2$
- **for** $i = 1 \to n+1$ **do**
  - $(x||w) = \pi(x||w)$
  - $m_i = x \oplus c_i$
  - $x = c_i$
- $(x||w) = \pi(x||w)$; $T' = \lfloor x \rfloor_k$
- $X' = m_1||\dots||m_{n+1}$;
- **if** $T == T'$ **then**
  - **if** $\exists$ M *s.t.* M = checkout(X', r, k, ℓ) **then**
    - Return:M
  - **else**
    - Return: $\perp$
- **else**
  - $\perp$

SIGNCRYPT Security

Theorem

Given that

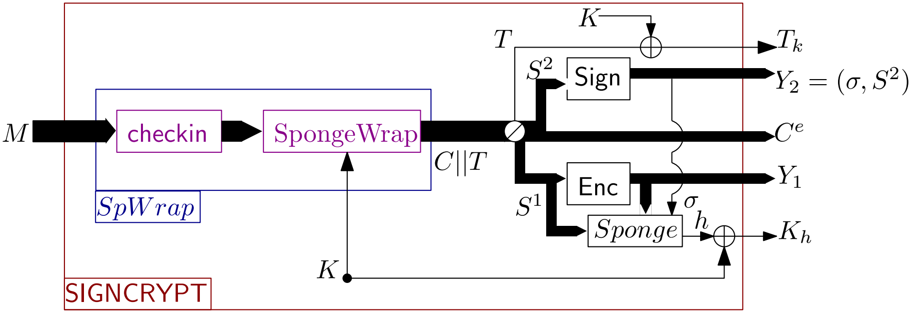
- *encryption is OW-PCA – one-way under plaintext checking attack and*
- *signature is deterministic* uUF-RMA *– universal unforgeable under random message attack*

then the signcryption is (IND-CCA/UF-AdA) *secure.*

Road Map

Generic SIGNCRYPT

SIGNCRYPT handles messages of arbitrary lengths



Security of Generic SIGNCRYPT

Theorem

Given that

- *encryption is OW-PCA and*
- *signature is* (uUF,suUF)-RMA

then the generic signcryption is IND-CCA/(UF,sUF)-AdA *secure.*

Unforgeability of SIGNCRYPT

ENCRYPT(↓) \ SIGN(→)		uUF-RMA	suUF-RMA
Deterministic	OW-CPA	UF-AdA	sUF-AdA
Probabilistic	OW-PCA	UF-AdA	UF-AdA

Privacy of SIGNCRYPT

Sign(↓) \ Encrypt(→)		OW-PCA
Deterministic	uUF-RMA	IND-CCA
	suUF-RMA	IND-CCA
Probabilistic	uUF-RMA	✗
	suUF-RMA	IND-CCA

Conclusions

Generic SIGNCRYPT has the following advantages:

- strong security from weaker components (security amplification)
- sponge structure provides efficient pre-processing of messages
- SIGNCRYPT is a template for practical implementation (plug and play)
- generic SIGNCRYPT allows to signcrypt messages of arbitrary lengths (consistent with KEM/DEM)
- generic SIGNCRYPT provides a tool for secure streaming (arbitrary long messages)

The full details can be found in [2].

References

[1] Jee Hea An, Yevgeniy Dodis, and Tal Rabin.
On the security of joint signature and encryption.
In *EUROCRYPT 2002, Amsterdam, The Netherlands*. Springer, 2002.

[2] Tarun Kumar Bansal, Xavier Boyen, and Josef Pieprzyk.
Signcryption Schemes with Insider Security in iIdeal Permutation Model.
J. Math. Cryptology, 2019.

[3] Yevgeniy Dodis, Michael J. Freedman, Stanislaw Jarecki, and Shabsi Walfish.
Versatile padding schemes for joint signature and encryption.
In *ACM-CCS 2004, Washington, DC, USA*. ACM, 2004.

[4] Yevgeniy Dodis, Michael J. Freedman, and Shabsi Walfish.
Parallel signcryption with oaep, pss-r, and other feistel paddings, 2003.
`http://eprint.iacr.org/2003/043`.

[5] Josef Pieprzyk and David Pointcheval.
Parallel authentication and public-key encryption.
In *ACISP 2003, Wollongong, Australia*. Springer, 2003.

Thank You