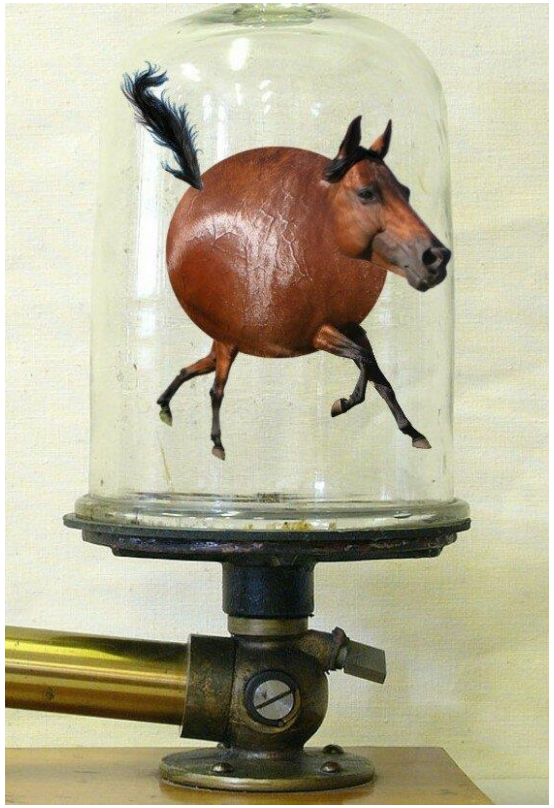
Attacks on authenticated key establishment protocols with forcing the public ephemeral values

Alekseev Evgeny, Kyazhin Sergey, Smyshlyaev Stanislav
CryptoPro LLC

CRYPTOPRO

2024 CTCRYPT

Security Models in Cryptography



Cryptanalysis steps:

1) Identify a relevant security model (based on expert experience)
2) Describe the model formally
3) Get security estimation within a formal model

Phong Q. Nguyen:

«There are a lot of similarities between cryptology and physics. Both use a lot of mathematics, but neither is part of mathematics.»

On importance of correct definition of security model:

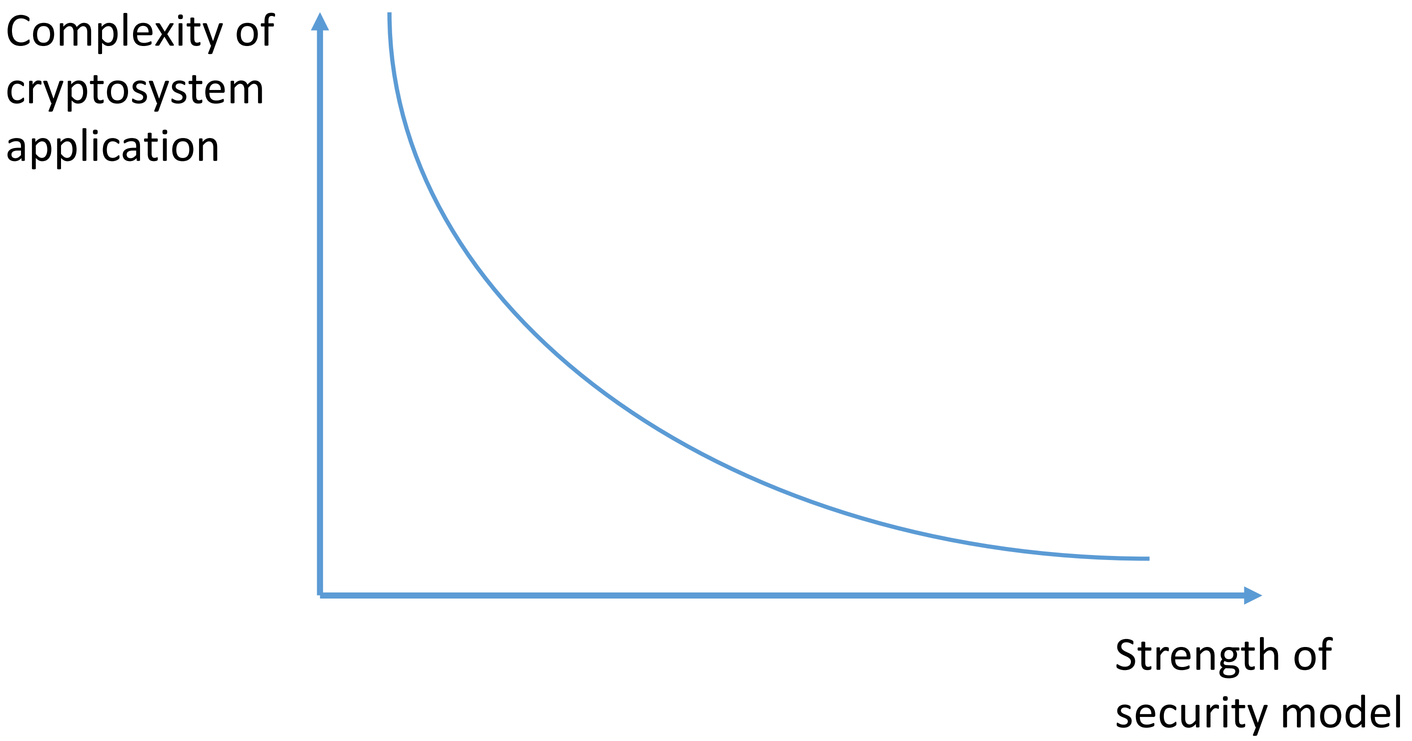
- Alekseev E.K., “What can go wrong if you use cryptography incorrectly”, CTCrypt 2019
- Degabriele J.P., Paterson K., Watson G. “Provable Security in the Real World”

CRYPTOPRO

Sources of Adversary Capabilities

Source of adversary capabilities:

- how cryptosystem is used/supposed to be used in practice



Attack on SIGMA

Public ephemeral values:

- appears during the protocol execution
- transmitted over the channel

Examples:

- client_random, server_random in TLS
- ephemeral public keys in any DH-based AKE

$$\mathbf{A} : sk_A^s, pk_A^s \qquad\qquad \mathbf{B} : sk_B^s, pk_B^s$$

$$e_A \leftarrow sMEM$$

$$\underline{E_A \leftarrow MEM} \quad \xrightarrow{\boxed{E_A}} \quad e_B \leftarrow sMEM$$

$$\underline{E_B \leftarrow MEM}$$

$$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A)$$

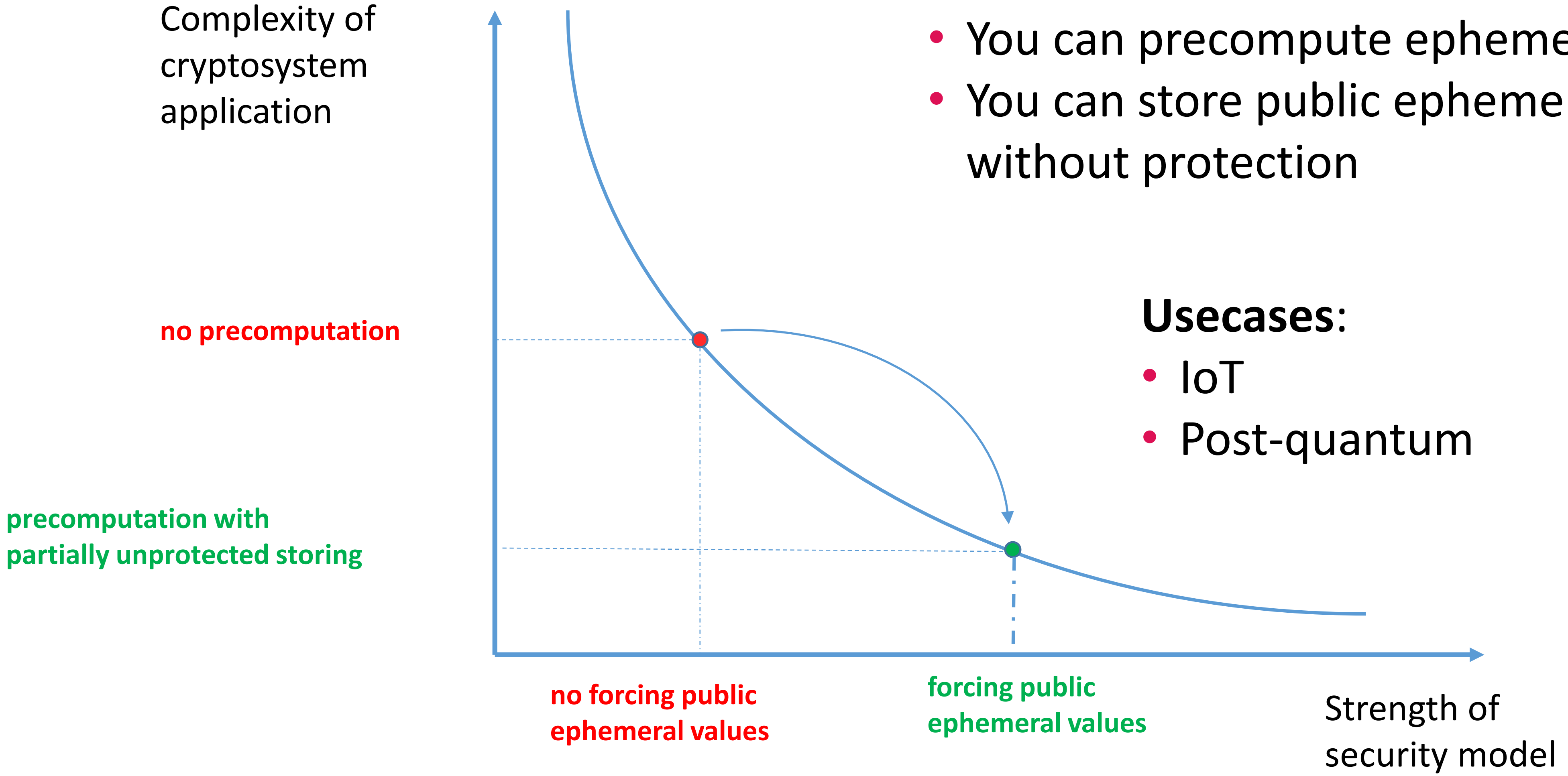
$$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B)$$

$$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot E_B) \quad \xleftarrow{B, \boxed{E_B}, \sigma_B, \tau_B} \quad \tau_B \leftarrow \mathsf{MAC}_{K^a}(B)$$

Forcing the public ephemeral values

Benefit:
- You can precompute ephemeral values
- You can store public ephemeral values without protection

Usecases:
- IoT
- Post-quantum



Attacks on AKE-protocols

Types of protocols under consideration (based on types of long-term keys used):

- Signature
- Scalar
- KEM (Key Encapsulation Mechanism)

Implemented threats:

- AUTH – adversary impersonate one of participants
- MITM – adversary impersonate both participants
- KCI – adversary impersonate some participant knowing the other participant's long-term key
- PFS – adversary gets the keys of previously established sessions after getting some participant’s long-term key
- SEC – adversary gets the session key established by some two honest participants

Attacks on AKE-protocols

Protocol type	Protocol	Result
Signature	SIG-DH+	AUTH
	SIGMA	AUTH, MITM
	Echinacea-3	AUTH, MITM
	SIGMA-R	AUTH
Scalar	TS3	AUTH
	CF	AUTH
	SK6	KCI, PFS, SEC
KEM	BKM-KK	AUTH

Notations: «AKE Zoo: 100 two-party protocols (to be continued)», ePrint paper 2023/1044.

Attacks on AKE-protocols

Protocol type	Protocol	Result
Signature	SIG-DH+	AUTH
	SIGMA	**AUTH**, MITM
	Echinacea-3	AUTH, MITM
	SIGMA-R	AUTH
Scalar	TS3	AUTH
	CF	**AUTH**
	SK6	KCI, PFS, SEC
KEM	**BKM-KK**	**AUTH**

Notations: «AKE Zoo: 100 two-party protocols (to be continued)», ePrint paper 2023/1044.

Attack on SIGMA

$\mathbf{A} : sk^s_A, pk^s_A$		$\mathbf{B} : sk^s_B, pk^s_B$
$e_A \leftarrow sMEM$		
$E_A \leftarrow MEM$	$\xrightarrow{E_A}$	$e_B \leftarrow sMEM$
	$\boxed{E'_B}$	$\cancel{E_B} \leftarrow MEM$
		$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
		$\sigma_B \leftarrow \mathsf{Sig}_{sk^s_B}(E_A, E_B)$
$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot E_B)$	$\xleftarrow{B, E_B, \sigma_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(B)$
Verify σ_B, τ_B		
$\sigma_A \leftarrow \mathsf{Sig}_{sk^s_A}(E_B, E_A)$		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(A)$	$\xrightarrow{A, \sigma_A, \tau_A}$	Verify σ_A, τ_A
return K		**return** K

Attack on SIGMA

$\mathbf{A} : sk_A^s, pk_A^s$		$\mathbf{B} : sk_B^s, pk_B^s$
$e_A \leftarrow sMEM$		
$E_A \leftarrow MEM$	$\xrightarrow{\quad E_A \quad}$	$e_B \leftarrow sMEM$
	$\boxed{E'_B}$	$\cancel{E_B} \leftarrow MEM$
		$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A \boxed{E'_B}$
$K, K^a \leftarrow \mathsf{KDF}(e_A \cdot \boxed{E'_B}$	$\xleftarrow{\quad B \boxed{E'_B} \sigma_B, \tau_B \quad}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(B)$
Verify σ_B, τ_B		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(\boxed{E'_B} E_A)$		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(A)$	$\xrightarrow{\quad A, \sigma_A, \tau_A \quad}$	Verify σ_A, τ_A
return K		**return** K

Attack on SIGMA

$\mathbf{A} : sk_A^s, pk_A^s$		$\mathbf{B} : sk_B^s, pk_B^s$
$e_A \leftarrow sMEM$		
$E_A \leftarrow MEM$	$\xrightarrow{\quad E_A \quad}$	$e_B \leftarrow sMEM$
	$\boxed{E'_B}$	$\cancel{E_B} \leftarrow MEM$
		$K, \underline{K^a} \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
		$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, \boxed{E'_B})$
$\boxed{\hat{K}, \hat{K}^a} \leftarrow \mathsf{KDF}(e_A \cdot \boxed{E'_B})$	$\xleftarrow{\quad B, \boxed{E'_B}, \sigma_B, \tau_B \quad}$	$\underline{\tau_B} \leftarrow \mathsf{MAC}_{K^a}(B)$
Verify $\sigma_B, \underline{\tau_B}$		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(\boxed{E'_B}, E_A)$		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(A)$	$\xrightarrow{\quad A, \sigma_A, \tau_A \quad}$	Verify σ_A, τ_A
return K		**return** K

Attack on SIGMA

$\mathbf{A} : sk_A^s, pk_A^s$		$\mathbf{B} : sk_B^s, pk_B^s$
$e_A \leftarrow sMEM$		
$E_A \leftarrow MEM$	$\xrightarrow{E_A}$	$e_B \leftarrow sMEM$
	$\boxed{E'_B}$	$\cancel{E_B} \leftarrow MEM$
		$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
	$\boxed{\tau'_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, \boxed{E'_B})$
$\boxed{\hat{K}, \hat{K}^a} \leftarrow \mathsf{KDF}(e_A \cdot \boxed{E'_B})$	$\xleftarrow{B, \boxed{E'_B}, \sigma_B, \cancel{\tau_B}}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(B)$
Verify $\sigma_B, \boxed{\tau'_B}$	$\boxed{\hat{K}, \hat{K}^a \leftarrow \mathsf{KDF}(e'_B \cdot E_A)}$	
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(\boxed{E'_B}, E_A)$		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(A)$	$\xrightarrow{A, \sigma_A, \tau_A}$	Verify σ_A, τ_A
return K		**return** K

Attack on SIGMA

$\mathbf{A} : sk_A^s, pk_A^s$		$\mathbf{B} : sk_B^s, pk_B^s$
$e_A \leftarrow sMEM$		
$E_A \leftarrow MEM$	$\xrightarrow{E_A}$	$e_B \leftarrow sMEM$
	$\boxed{E'_B}$	$\cancel{E_B} \leftarrow MEM$
		$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
	$\boxed{\tau'_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, \boxed{E'_B})$
$\boxed{\hat{K}, \hat{K}^a} \leftarrow \mathsf{KDF}(e_A \cdot \boxed{E'_B})$	$\xleftarrow{B, \boxed{E'_B}, \sigma_B, \cancel{\tau_B}}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(B)$
Verify $\sigma_B, \boxed{\tau'_B}$	$\boxed{\hat{K}, \hat{K}^a \leftarrow \mathsf{KDF}(e'_B \cdot E_A)}$	
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(\boxed{E'_B}, E_A)$		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(A)$	$\xrightarrow{A, \cancel{\sigma_A}, \tau_A}$	$\cancel{\text{Verify } \sigma_A, \tau_A}$
return K		$\cancel{\textbf{return } K}$

Attack on SIGMA

$\mathbf{A} : sk_A^s, pk_A^s$		$\mathbf{B} : sk_B^s, pk_B^s$
$e_A \leftarrow sMEM$		
$E_A \leftarrow MEM$	$\xrightarrow{E_A}$	$e_B \leftarrow sMEM$
	$\boxed{E'_B}$	$\cancel{E_B} \leftarrow MEM$
		$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
	$\boxed{\tau'_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, \boxed{E'_B})$
$\boxed{\hat{K}, \hat{K}^a} \leftarrow \mathsf{KDF}(e_A \cdot \boxed{E'_B})$	$\xleftarrow{B, \boxed{E'_B}, \sigma_B, \cancel{\tau_B}}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(B)$
Verify $\sigma_B, \boxed{\tau'_B}$	$\boxed{\hat{K}, \hat{K}^a \leftarrow \mathsf{KDF}(e'_B \cdot E_A)}$	
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(\boxed{E'_B}, E_A)$		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(A)$	$\xrightarrow{\cancel{A, \sigma_A, \tau_A}}$	$\cancel{\text{Verify } \sigma_A, \tau_A}$
return $\boxed{\hat{K}}$		$\cancel{\textbf{return } K}$

Attack on SIGMA

A : sk^s_A, pk^s_A		**B** : sk^s_B, pk^s_B
$e_A \leftarrow sMEM$		
$E_A \leftarrow MEM$	$\xrightarrow{E_A}$	$e_B \leftarrow sMEM$
	$\boxed{E'_B}$	$\cancel{E_B} \leftarrow MEM$
		$K, K^a \leftarrow \mathsf{KDF}(e_B \cdot E_A)$
	$\boxed{\tau'_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk^s_B}(E_A, \boxed{E'_B})$
$\boxed{\hat{K}, \hat{K}^a} \leftarrow \mathsf{KDF}(e_A \cdot \boxed{E'_B})$	$\xleftarrow{B, \boxed{E'_B}, \sigma_B, \cancel{\tau_B}}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a}(B)$
Verify $\sigma_B, \boxed{\tau'_B}$	$\boxed{\hat{K}, \hat{K}^a \leftarrow \mathsf{KDF}(e'_B \cdot E_A)}$	
$\sigma_A \leftarrow \mathsf{Sig}_{sk^s_A}(\boxed{E'_B}, E_A)$		
$\tau_A \leftarrow \mathsf{MAC}_{K^a}(A)$	$\xrightarrow{A, \cancel{\sigma_A, \tau_A}}$	$\cancel{\text{Verify } \sigma_A, \tau_A}$
return $\boxed{\hat{K}}$		$\cancel{\textbf{return } K}$

Attack on CF

A : $\boxed{(x_A, X_A)}$ (sk_A^s, pk_A^s)		**B** : $\boxed{(x_B, X_B)}$ (sk_B^s, pk_B^s)
$e_A \leftarrow sMEM$		
$\underline{E_A \leftarrow MEM}$		
$\sigma_A \leftarrow \mathsf{Sig}_{sk_A^s}(E_A)$	$\xrightarrow{A, \boxed{E_A}, \sigma_A}$	Verify σ_A
		$e_B \leftarrow sMEM$
		$\underline{E_B \leftarrow MEM}$
Verify σ_B	$\xleftarrow{B, \boxed{E_B}, \sigma_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_B)$
$W \leftarrow (e_A + x_A) \cdot (E_B + X_B)$		$W \leftarrow (e_B + x_B) \cdot (E_A + X_A)$
$K \leftarrow \mathsf{KDF}(A, B, W, E_A)$		$K \leftarrow \mathsf{KDF}(A, B, W, E_A)$
return K		**return** K

Attack on CF

$\boxed{E'_A = -X_A + P}$

$$
\begin{array}{lcl}
\mathbf{A}: \boxed{(x_A, X_A)}\ (sk^s_A, pk^s_A) & & \mathbf{B}: \boxed{(x_B, X_B)}\ (sk^s_B, pk^s_B) \\
\hline
e_A \leftarrow sMEM & & \\
\cancel{E_A} \leftarrow MEM & & \\
\sigma_A \leftarrow \mathsf{Sig}_{sk^s_A}(E_A) & \xrightarrow{A, E_A, \sigma_A} & \text{Verify } \sigma_A \\
& & e_B \leftarrow sMEM \\
& & E_B \leftarrow MEM \\
\text{Verify } \sigma_B & \xleftarrow{B, E_B, \sigma_B} & \sigma_B \leftarrow \mathsf{Sig}_{sk^s_B}(E_B) \\
W \leftarrow (e_A + x_A)\cdot(E_B + X_B) & & W \leftarrow (e_B + x_B)\cdot(E_A + X_A) \\
K \leftarrow \mathsf{KDF}(A, B, W, E_A) & & K \leftarrow \mathsf{KDF}(A, B, W, E_A) \\
\mathbf{return}\ K & & \mathbf{return}\ K
\end{array}
$$

Attack on CF

$\boxed{E'_A = -X_A + P}$

$\mathbf{A}: \boxed{(x_A, X_A)}, (sk^s_A, pk^s_A)$		$\mathbf{B}: \boxed{(x_B, X_B)}, (sk^s_B, pk^s_B)$
$e_A \leftarrow sMEM$		
$\cancel{E_A} \leftarrow MEM$		
$\sigma_A \leftarrow \mathsf{Sig}_{sk^s_A}(\boxed{E'_A})$	$\xrightarrow{A, \boxed{E'_A}, \sigma_A}$	Verify σ_A
		$e_B \leftarrow sMEM$
		$E_B \leftarrow MEM$
Verify σ_B	$\xleftarrow{B, E_B, \sigma_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk^s_B}(E_B)$
$W \leftarrow (e_A + x_A) \cdot (E_B + X_B)$		$W \leftarrow (e_B + x_B) \cdot (\boxed{E'_A} + X_A)$
$K \leftarrow \mathsf{KDF}(A, B, W, E_A)$		$K \leftarrow \mathsf{KDF}(A, B, W, \boxed{E'_A})$
return K		**return** K

Attack on CF

$\boxed{E'_A = -X_A + P}$

$\mathbf{A} : \boxed{(x_A, X_A)}\ (sk^s_A, pk^s_A)$		$\mathbf{B} : \boxed{(x_B, X_B)}\ (sk^s_B, pk^s_B)$
$e_A \leftarrow sMEM$		
$\cancel{E_A} \leftarrow MEM$		
$\sigma_A \leftarrow \mathsf{Sig}_{sk^s_A}(\boxed{E'_A})$	$\xrightarrow{A,\ \boxed{E'_A},\ \sigma_A}$	Verify $\underline{\sigma_A}$
		$e_B \leftarrow sMEM$
		$E_B \leftarrow MEM$
Verify σ_B	$\xleftarrow{B,\ E_B,\ \sigma_B}$	$\sigma_B \leftarrow \mathsf{Sig}_{sk^s_B}(E_B)$
$W \leftarrow (e_A + x_A) \cdot (E_B + X_B)$		$W \leftarrow (e_B + x_B) \cdot (\boxed{E'_A} + X_A)$
$K \leftarrow \mathsf{KDF}(A, B, W, E_A)$		$K \leftarrow \mathsf{KDF}(A, B, W, \boxed{E'_A})$
return K		**return** $\boxed{\hat{K}}$

$$\boxed{\begin{aligned} W' &\leftarrow E_B + X_B \\ \hat{K} &\leftarrow \mathsf{KDF}(A, B, W', E'_A) \end{aligned}}$$

Attack on BKM-KK (2023, post-quantum!)

$\mathbf{A} : sk_A^k, pk_A^k$		$\mathbf{B} : sk_B^k, pk_B^k$
$C_A, K_A^a \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{pk_B^k}()$	$\xrightarrow{\quad C_A \quad}$	$\widetilde{sk_B^k} \leftarrow sMEM$
		$\underline{\widetilde{pk_B^k} \leftarrow MEM}$
		$C_B, K_B^a \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{pk_A^k}()$
		$K_A^a \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{sk_B^k}(C_A)$
Verify τ_B	$\xleftarrow{\quad \boxed{\widetilde{pk_B^k},} C_B, \tau_B \quad}$	$\tau_B \leftarrow \mathsf{MAC}_{K_A^a}(\widetilde{pk_B^k}, C_A, C_B, A)$
$K_B^a \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{sk_A^k}(C_B)$		
$C_A^*, K \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{\widetilde{pk_B^k}}()$		
$\tau_A \leftarrow \mathsf{MAC}_{K_B^a}(C_A^*, C_A, C_B, B)$	$\xrightarrow{\quad C_A^*, \tau_A \quad}$	Verify τ_A
		$K \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{\widetilde{sk_B^k}}(C_A^*)$
return K		**return** K

Attack on BKM-KK (2023, post-quantum!)

$\mathbf{A} : sk^k_A, pk^k_A$		$\mathbf{B} : sk^k_B, pk^k_B$
$C_A, K^a_A \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{pk^k_B}()$	$\xrightarrow{C_A}$	$\widetilde{sk}^k_B \leftarrow sMEM$
	$\boxed{\widetilde{pk}^k}$	$\cancel{\widetilde{pk}^k_B} \leftarrow MEM$
		$C_B, K^a_B \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{pk^k_A}()$
		$K^a_A \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{sk^k_B}(C_A)$
Verify τ_B	$\xleftarrow{\widetilde{pk}^k_B, C_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K^a_A}(\widetilde{pk}^k_B, C_A, C_B, A)$
$K^a_B \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{sk^k_A}(C_B)$		
$C^*_A, K \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{\widetilde{pk}^k_B}()$		
$\tau_A \leftarrow \mathsf{MAC}_{K^a_B}(C^*_A, C_A, C_B, B)$	$\xrightarrow{C^*_A, \tau_A}$	Verify τ_A
		$K \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{\widetilde{sk}^k_B}(C^*_A)$
return K		**return** K

Attack on BKM-KK (2023, post-quantum!)

$\mathbf{A} : sk_A^k, pk_A^k$		$\mathbf{B} : sk_B^k, pk_B^k$
$C_A, K_A^a \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{pk_B^k}()$	$\xrightarrow{C_A}$	$\widetilde{sk}_B^k \leftarrow sMEM$
	$\boxed{\widetilde{pk}^k}$	$\cancel{\widetilde{pk}_B^k} \leftarrow MEM$
		$C_B, K_B^a \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{pk_A^k}()$
		$K_A^a \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{sk_B^k}(C_A)$
Verify τ_B	$\xleftarrow{\boxed{\widetilde{pk}^k}, C_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K_A^a}(\boxed{\widetilde{pk}^k,} C_A, C_B, A)$
$K_B^a \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{sk_A^k}(C_B)$		
$C_A^*, K \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{\boxed{\widetilde{pk}^k}}()$		
$\tau_A \leftarrow \mathsf{MAC}_{K_B^a}(C_A^*, C_A, C_B, B)$	$\xrightarrow{C_A^*, \tau_A}$	Verify τ_A
		$K \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{\widetilde{sk}_B^k}(C_A^*)$
return K		**return** K

Attack on BKM-KK (2023, post-quantum!)

$\mathbf{A}: sk_A^k, pk_A^k$		$\mathbf{B}: sk_B^k, pk_B^k$
$C_A, K_A^a \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{pk_B^k}()$	$\xrightarrow{\quad C_A \quad}$	$\widetilde{sk_B^k} \leftarrow sMEM$
	$\boxed{\widetilde{pk^k}}$	$\cancel{\widetilde{pk_B^k}} \leftarrow MEM$
		$C_B, K_B^a \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{pk_A^k}()$
		$K_A^a \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{sk_B^k}(C_A)$
Verify τ_B	$\xleftarrow{\quad \boxed{\widetilde{pk^k}}, C_B, \tau_B \quad}$	$\tau_B \leftarrow \mathsf{MAC}_{K_A^a}\boxed{(\widetilde{pk^k},} C_A, C_B, A)$
$K_B^a \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{sk_A^k}(C_B)$		
$C_A^*, K \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{\boxed{\widetilde{pk^k}}}()$		
$\tau_A \leftarrow \mathsf{MAC}_{K_B^a}(C_A^*, C_A, C_B, B)$	$\xrightarrow{\quad C_A^*, \tau_A \quad}$	Verify τ_A
	$\boxed{K \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{\widetilde{sk^k}}(C_A^*)}$	$K \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{\widetilde{sk_B^k}}(C_A^*)$
return K		**return** K

Attack on BKM-KK (2023, post-quantum!)

$\mathbf{A} : sk_A^k, pk_A^k$		$\mathbf{B} : sk_B^k, pk_B^k$
$C_A, K_A^a \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{pk_B^k}()$	$\xrightarrow{C_A}$	$\widetilde{sk_B^k} \leftarrow sMEM$
	$\boxed{\widetilde{pk^k}}$	$\widetilde{\cancel{pk_B^k}} \leftarrow MEM$
		$C_B, K_B^a \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{pk_A^k}()$
		$K_A^a \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{sk_B^k}(C_A)$
Verify τ_B	$\xleftarrow{\boxed{\widetilde{pk^k}}, C_B, \tau_B}$	$\tau_B \leftarrow \mathsf{MAC}_{K_A^a}(\boxed{\widetilde{pk^k},} C_A, C_B, A)$
$K_B^a \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{sk_A^k}(C_B)$		
$C_A^*, K \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{\boxed{\widetilde{pk^k}}}()$		
$\tau_A \leftarrow \mathsf{MAC}_{K_B^a}(C_A^*, C_A, C_B, B)$	$\xrightarrow{C_A^*, \tau_A}$	Verify τ_A
	$\boxed{K \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{\widetilde{sk^k}}(C_A^*)}$	$K \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{\widetilde{sk_B^k}}(C_A^*)$
return K		**return** K

Protection for signature-based protocols

To sign values computed using ephemeral private key

$$\sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B) \Rightarrow \sigma_B \leftarrow \mathsf{Sig}_{sk_B^s}(E_A, E_B, \mathsf{MAC}_{K^a}(B))$$

SIGMA **SIGMA-opt1**

Protection for scalar-based protocols

To compute key for authentication tags using combinations of long-term and ephemeral keys without simple algebraic relations

$$W \leftarrow (e_B + x_B) \cdot (E_A + X_A)$$
$$K \leftarrow \mathsf{KDF}(A, B, W, E_A)$$

CF

$$Q \leftarrow e_B \cdot X_A$$
$$R \leftarrow x_B \cdot E_A$$
$$K, K^a \leftarrow \mathsf{KDF}(Q, R, A, B)$$

Limonnik-3

Protection for KEM-based protocols

To compute key for authentication tags using results of decapsulation on long-term keys

$$K \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{\widetilde{sk^k_B}}(C^*_A)$$

BKM-KK

$$\widetilde{K_B} \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{\widetilde{sk^k_A}}(\widetilde{C_B})$$

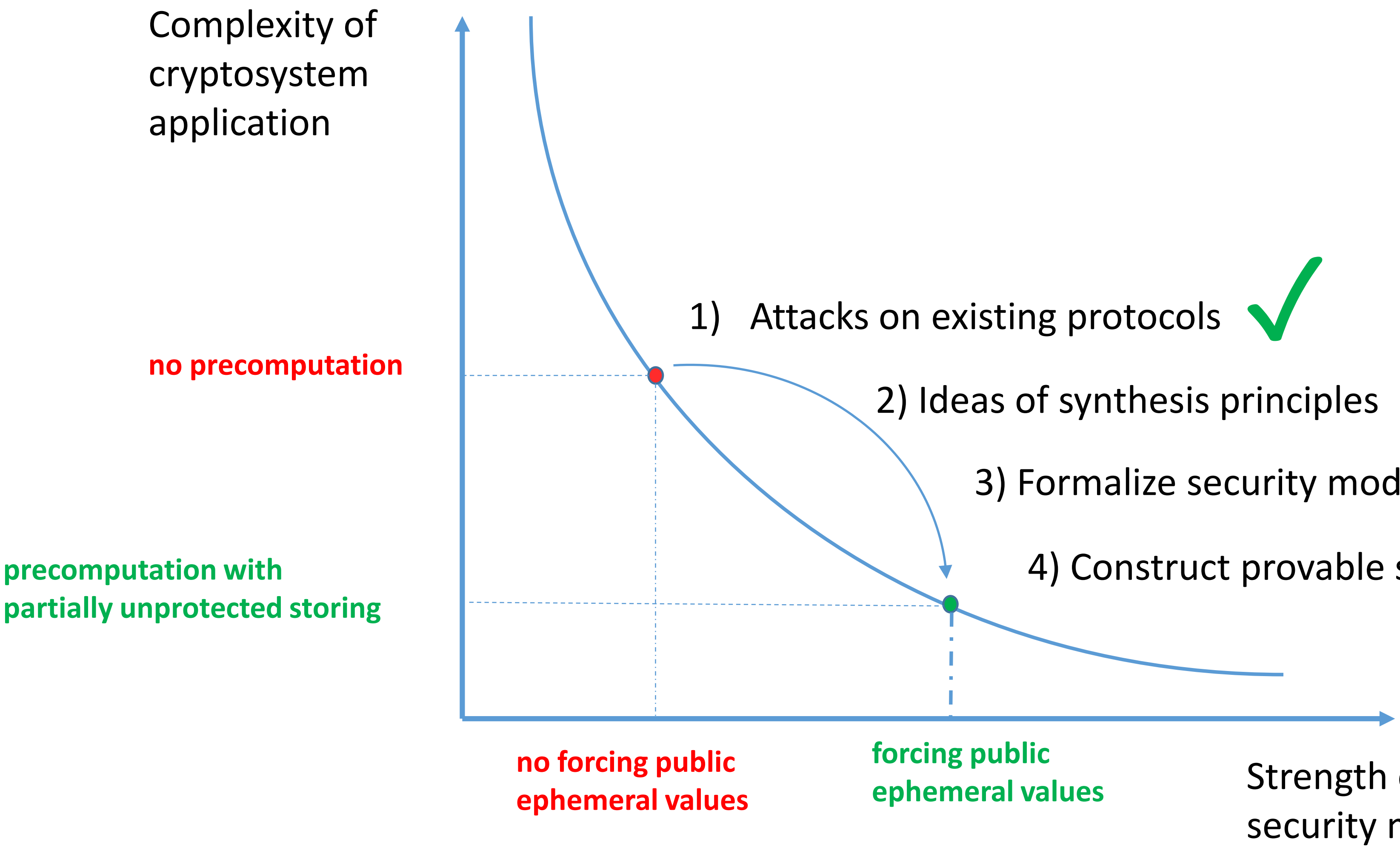
$$C_A, K_A \leftarrow \mathcal{KEM}.\mathsf{Encaps}_{pk^k_B}(\,)$$

$$K_B \leftarrow \mathcal{KEM}.\mathsf{Decaps}_{sk^k_A}(C_B)$$

$$K, K^a \leftarrow \mathsf{KDF}(\widetilde{K_B}, K_A, K_B)$$

KEMTLS

Conclusion and open questions



1) Attacks on existing protocols ✓
2) Ideas of synthesis principles ✓
3) Formalize security model ?
4) Construct provable secure protocols ?

Thank you for your attention!

alekseev@cryptopro.ru

Attacks on AKE-protocols

Types of protocols under consideration (based on types of long-term keys used):
- Signature
- Scalar
- KEM (Key Encapsulation Mechanism)

Used capabilities:
- FPVi/FPVr – to force ephemeral public values (to initiator/to responder)
- AC – to change the messages, transmitted over the channel
- LKC – to compromise long-term key
- SKC – to compromise session key

Implemented threats:
- AUTH – adversary impersonate one of participants
- MITM – adversary impersonate both participants
- KCI – adversary impersonate some participant knowing the other participant's long-term key
- PFS – adversary gets the keys of previously established sessions after getting some participant’s long-term key
- SEC – adversary gets the session key established by some two honest participants