Two-party GOST in two parts: fruitless search and fruitful synthesis

Lidiia Nikiforova, Liliya Akhmetzyanova, Evgeny Alekseev,
Alexandra Babueva and Stanislav Smyshlyaev

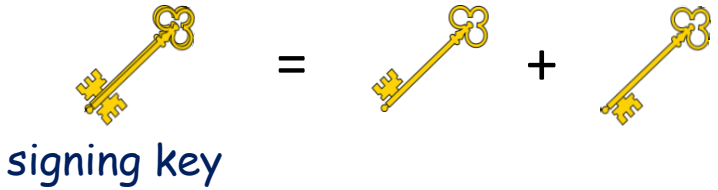
CryptoPro LLC

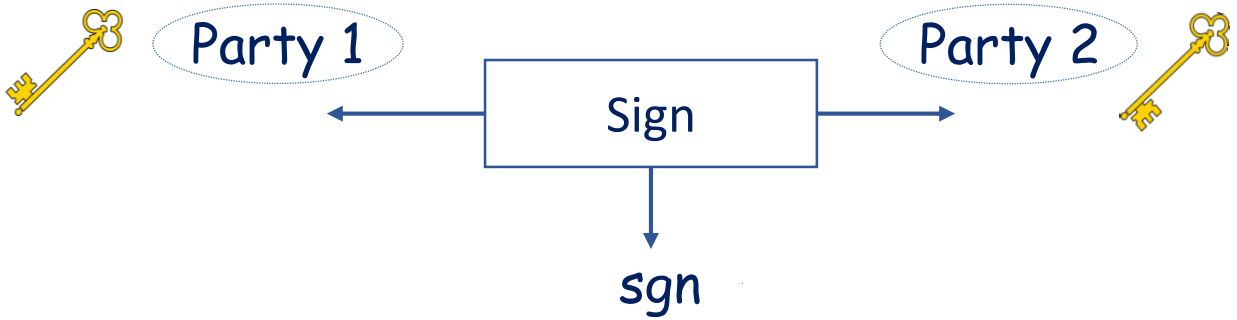
CRYPTOPRO

CTCrypt'2023

Two-party GOST…

Two-party signature

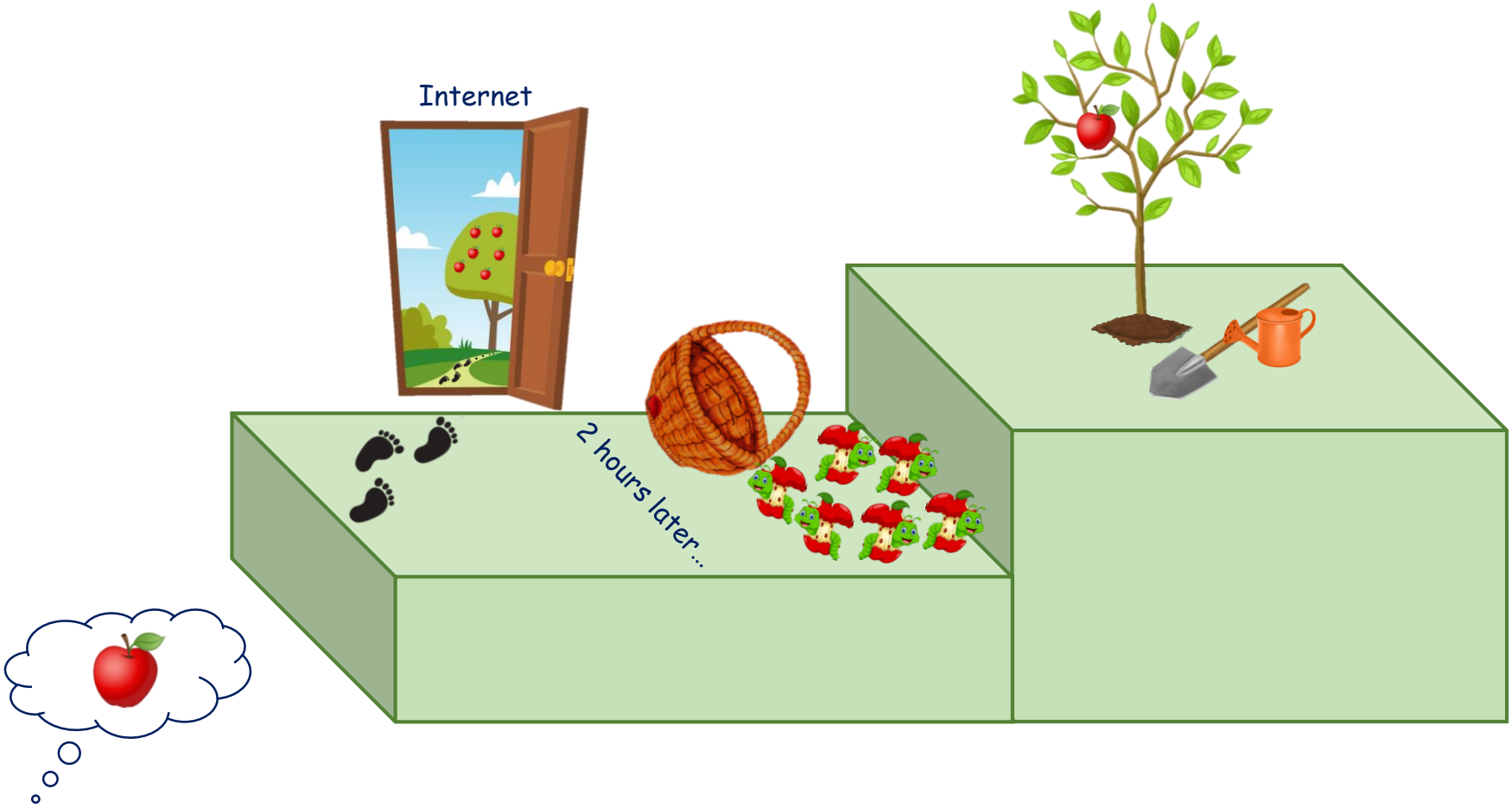




Additional conditions:

- Verification algorithm as in the GOST scheme
- No third trusted party in the key generating protocol
- Not use any non-standard cryptographic mechanisms

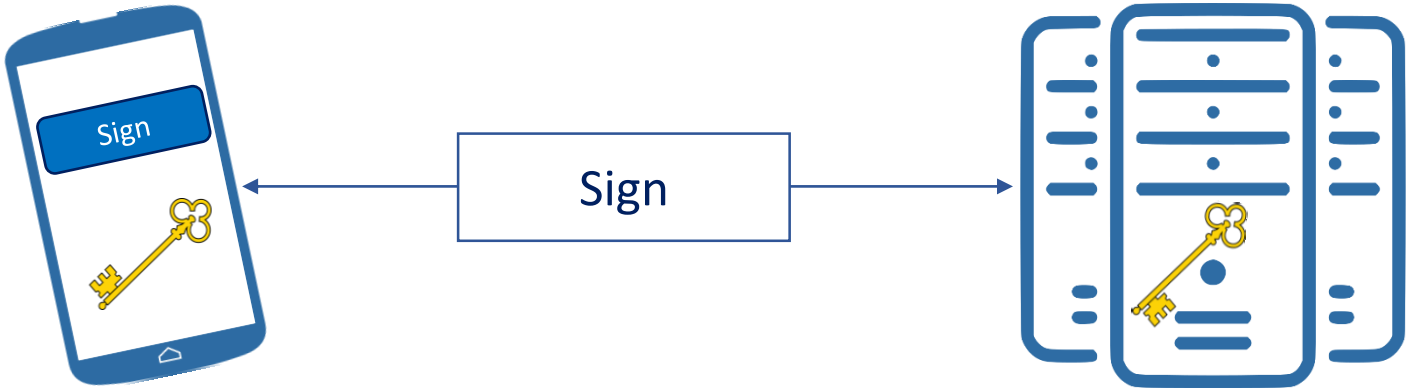
…fruitless search and fruitful synthesis



Practical problem

can sign undetectable

Practical problem



Active adversary

can't sign without the server

The server notifies and knows all signed messages

can't sign without the client

The content of the work

1. Search
2. Analysis
3. Design rationale
4. Synthesis
5. Cryptanalysis

… no more pictures in the rest of the talks…

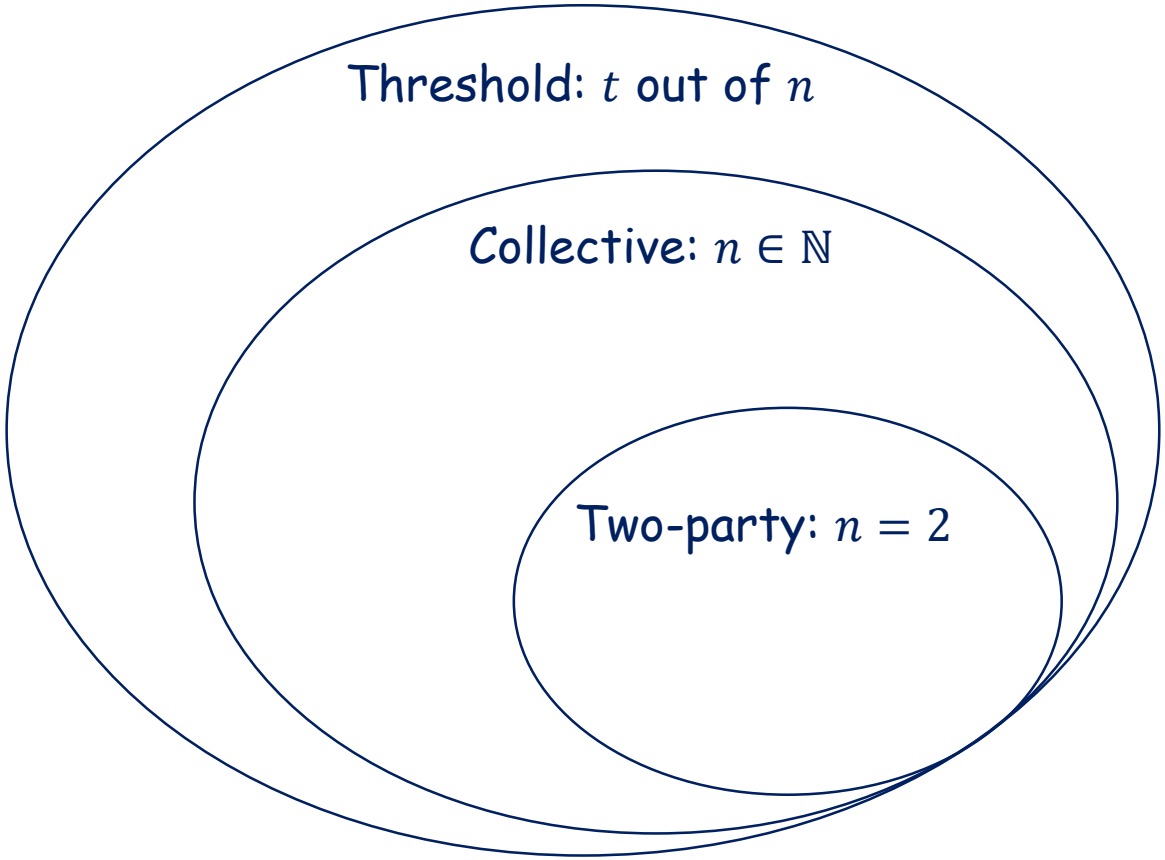
Search

Two-party signature scheme:

- KGen – an interactive key generation protocol that is run between a Party 1 and a Party 2
- Sign – an interactive signing protocol that is run between a Party 1 and a Party 2
- Verify – a (deterministic) verification algorithm

Search

Not only two-party schemes



Search

	2010	N.A. Moldovyan	«Theoretical minimum and digital signature algorithms»
	2010	Dzhunkovsky P. O., Ditenkova A. S.	«Threshold scheme of a digital signature with a shared secret based on GOST R 34.10-2001»
	2011	S. Kim, J. Kim, J. Cheon, S. Ju	«Threshold signature schemes for ElGamal variants»
	2016	A. Beresneva, A. Epishkina, O. Isupova, K. Kogos, M. Shimkiv	«Special digital signature schemes based on GOST R 34.10-2012»
	2020	Y. Zhang, M. Luo, K. Choo, L. Li, D. He	«Efficient and Secure Two-Party Distributed Signing Protocol for the GOST Signature Algorithm»
	2022	T. N. Kim, D.H. Ngoc, N. A. Moldovyan	«New Collective Signatures Based on the Elliptic Curve Discrete Logarithm Problem»

Search: checking of conditions

	2010	N.A. Moldovyan	«Theoretical minimum and digital signature algorithms»
	2010	Dzhunkov Ditenkova	
X	2011	S. Kim, J. Kim, J. Cheon, S. Ju	«Threshold signature schemes for ElGamal variants»
X	2016	A. Beresneva, A. Epishkina, O. Isupova, K. Kogos, M. Shimkiv	«Special digital signature schemes based on GOST R 34.10-2012»
	2020	Y. Zhang, K. Choo,	
	2022	T. N. Kim, D.H. Ngoc, N. A. Moldovyan	«New Collective Signatures Based on the Elliptic Curve Discrete Logarithm Problem»

Proven secure only against passive adversary

Third trusted party to form the signature

Design rationale

The GOST signature scheme:

KGen ( ): $d \xleftarrow{u} \mathbb{Z}_q^*, Q \leftarrow d \cdot P,$ return (d, Q)

Sign (d, m)

$e \leftarrow \mathrm{H}(m)$
$k \xleftarrow{u} \mathbb{Z}_q^*$
$r \leftarrow (k \cdot P).x \bmod q$
$s \leftarrow ke + dr$
return (r, s)

Secret parameters:

d – a signing key
k – an ephemeral value

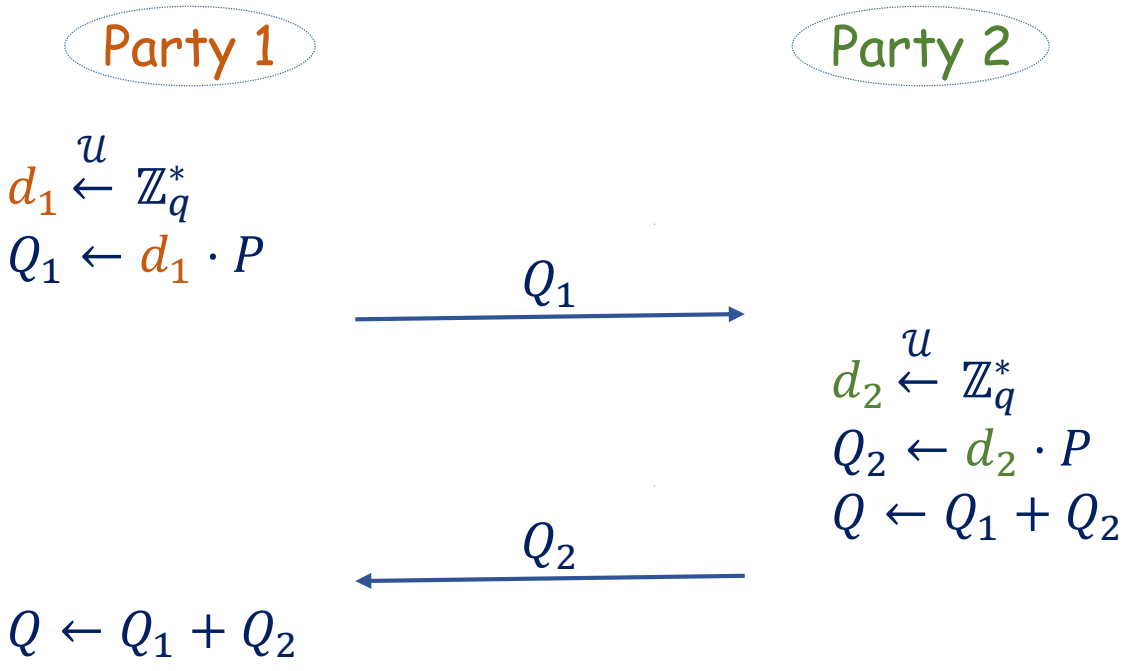
The signature equation is linear with respect to secret parameters

$$k = k_1 + k_2$$
$$d = d_1 + d_2$$

$r \leftarrow (k_1 \cdot P + k_2 \cdot P).x \bmod q$
$s \leftarrow (k_1 + k_2)e + (d_1 + d_2)r$

Design rationale: the key generation protocol

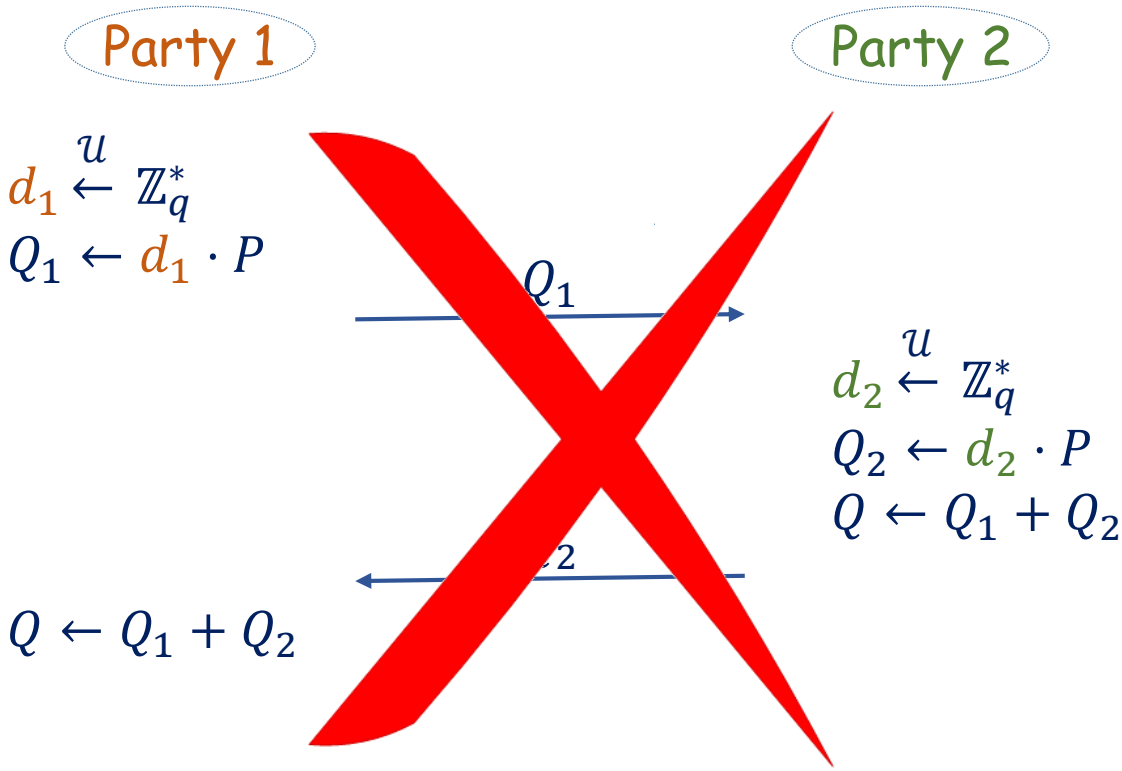
The naive version of the key generation protocol:



Q – a verifying key

Design rationale: the key generation protocol

The naive version of the key generation protocol:



It is not secure!

Design rationale: the key generation protocol

The naive version of the key generation protocol:

Party 1

$d_1 \xleftarrow{u} \mathbb{Z}_q^*$

$Q_1 \leftarrow d_1 \cdot P$

Q_1 →

$Q_2 \leftarrow P - Q_1$

$Q \leftarrow Q_1 + Q_2 = P$

← Q_2

$Q \leftarrow Q_1 + Q_2 = P$

The signing key $d = 1$

Search: the key generation protocol

?	2010	N.A. Moldovyan	«Theoretical minimum and digital signature algorithms»
?	2010	Dzhunkovsky P. O., Ditenkova A. S.	«Threshold scheme of a digital signature with a shared secret based on GOST R 34.10-2001»
X	2011	S. Kim, J. Kim, J. Cheon, S	«Threshold signature schemes for
X	2016	A E K. Kogos, M. Shimkiv	emes based on GOST R 34.10-2012»
	2020	Y. Zhang, M. Luo, K. Choo, L. Li, D. He	«Efficient and Secure Two-Party Distributed Signing Protocol for the GOST Signature Algorithm»
?	2022	T. N. Kim, D.H. Ngoc, N. A. Moldovyan	«New Collective Signatures Based on the Elliptic Curve Discrete Logarithm Problem»

There is no description of the distributed key generation protocol

Design rationale: the key generation protocol

One way to protect is to use a commitment scheme [1].

Commitment scheme:

- Cmt – a commitment generation algorithm
- Open – a (deterministic) commitment opening algorithm

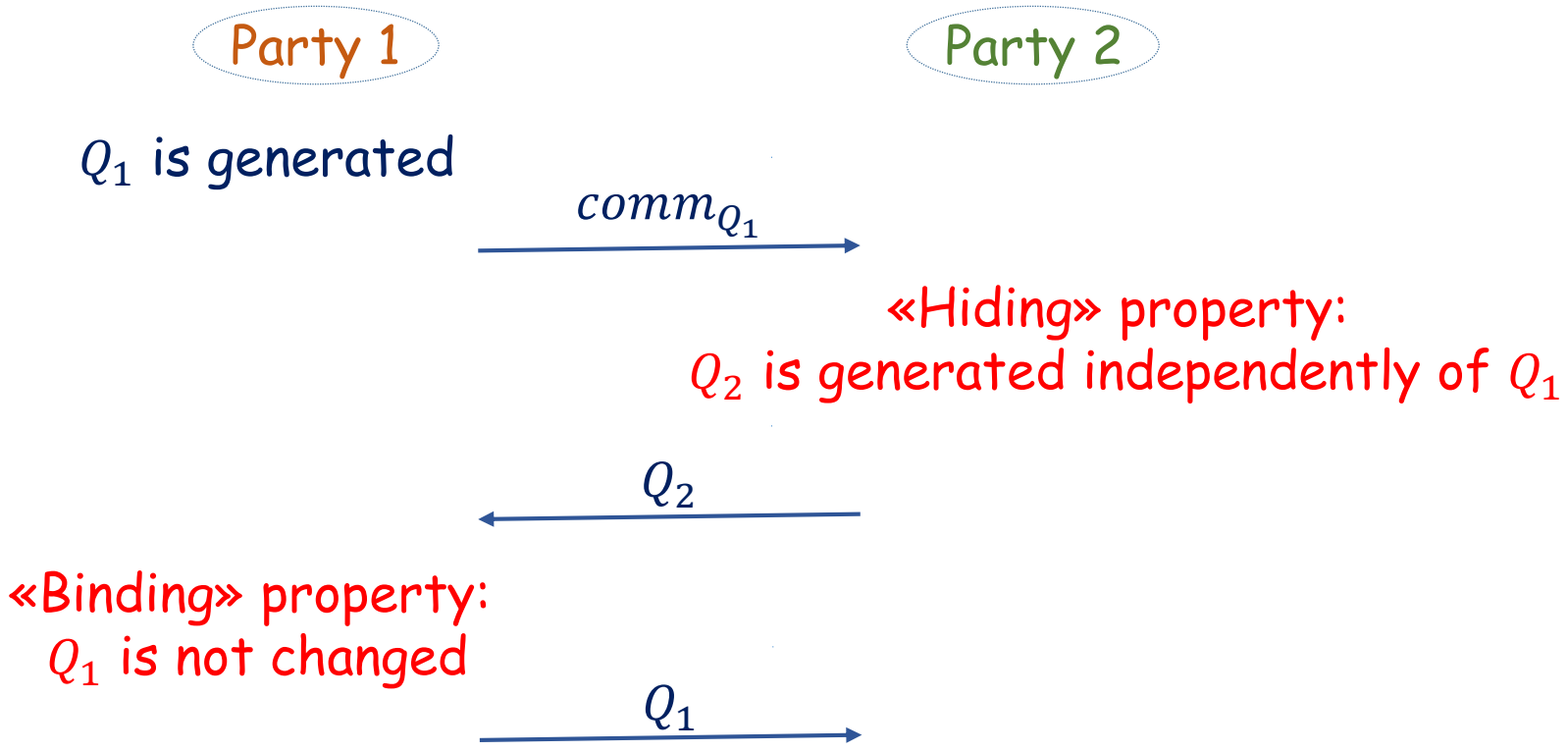
«Hiding» property: no one can learn any information, given only the commitment

«Binding» property: a party cannot change the value or statement after they have committed to it

[1] Nicolosi, Antonio and Krohn, Maxwell N and Dodis, Yevgeniy and Mazieres, David, "Proactive Two-Party Signatures for User Authentication,", NDSS, 2003.

Design rationale: the key generation protocol

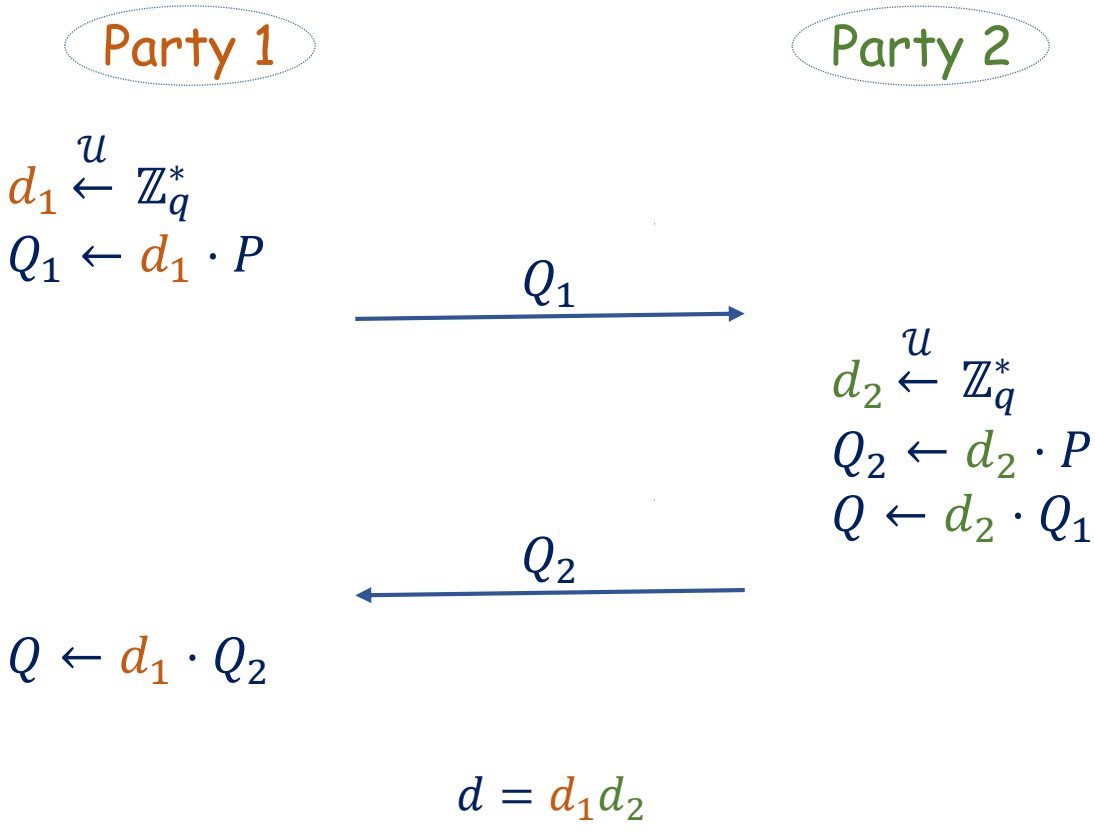
One way to protect is to use a commitment scheme [1]



[1] Nicolosi, Antonio and Krohn, Maxwell N and Dodis, Yevgeniy and Mazieres, David, "Proactive Two-Party Signatures for User Authentication,", NDSS, 2003.

Design rationale: the key generation protocol

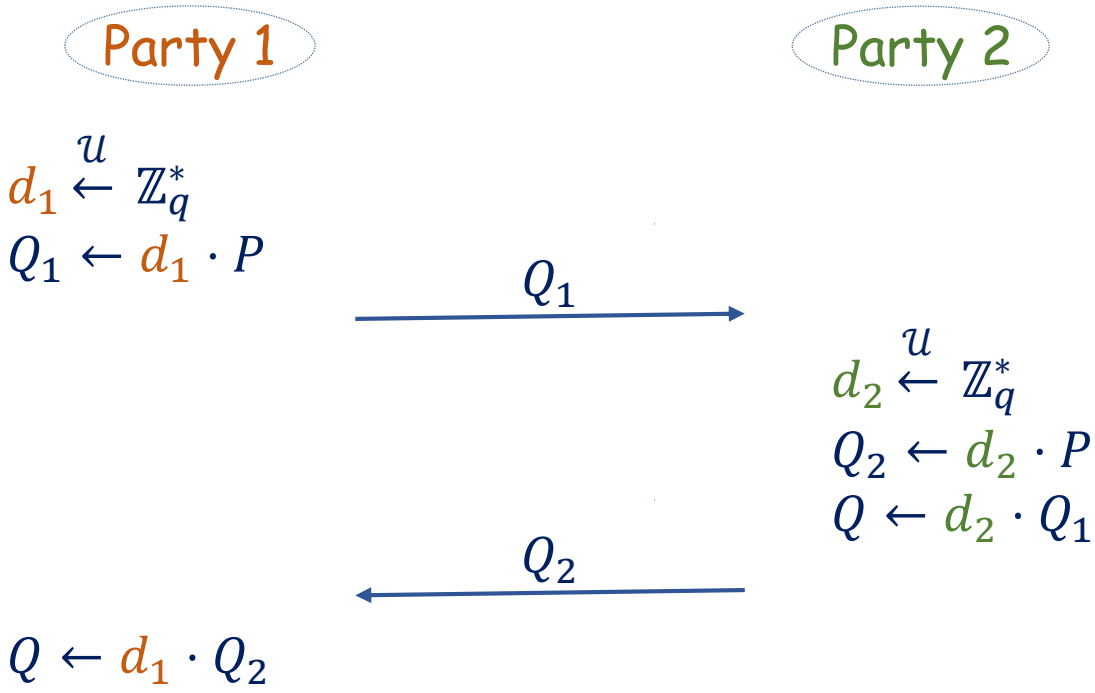
Another way to protect is to use the multiplicative method of the key sharing [2]



[2] Zhang, Yunru and Luo, Min and Choo, Kim-Kwang Raymond and Li, Li and He, Debiao, "Efficient and Secure Two-Party Distributed Signing Protocol for the GOST Signature Algorithm", … SocialSec 2020 …

Design rationale: the key generation protocol

Another way to protect is to use the multiplicative method of the key sharing [2]



There is no obvious way how to create a signature

Additively homomorphic encryption scheme is used in [2]

[2] Zhang, Yunru and Luo, Min and Choo, Kim-Kwang Raymond and Li, Li and He, Debiao, "Efficient and Secure Two-Party Distributed Signing Protocol for the GOST Signature Algorithm", … SocialSec 2020 …

Search: checking of conditions

?	2010	N.A. Moldovyan	«Theoretical minimum and digital signature algorithms»
?	2010	Dzhunkovsky P. O., Ditenkova A. S.	«Threshold scheme of a digital signature with a shared secret based on GOST R 34.10-2001»
X	2011	S. Kim, J. Kim, J. Cheon, S	«Threshold signature schemes for
X	2016	A E K. Kogos, M. Shimkiv	emes based on GOST R 34.10-2012»
X	2020	Y. Zhang, M. Luo, K. Choo, L. Li, D. He	«Efficient and Secure Two-Party Distributed Signing Protocol for the GOST Signature Algorithm»
?	2022	T. N. Kim, D.H. Ngoc, N. A. Moldovyan	«New Collective Signatures Based on the Elliptic Curve Discrete Logarithm Problem»

Additively homomorphic encryption is used

Search

Two-party signature scheme:

- KGen
- Sign
- Verify

Design rationale: the signing protocol

The naive version of the signing protocol:

Party 1		Party 2
d_1, Q, m		d_2, Q, m
$e \leftarrow \mathrm{H}(m)$		$e \leftarrow \mathrm{H}(m)$
$k_1 \overset{u}{\leftarrow} \mathbb{Z}_q^*$		
$R_1 \leftarrow k_1 \cdot P$		
	$R_1 \rightarrow$	
		$k_2 \overset{u}{\leftarrow} \mathbb{Z}_q^*$
		$R_2 \leftarrow k_2 \cdot P$
		$r \leftarrow (R_1 + R_2).x \bmod q$
		$s_2 \leftarrow k_2 e + d_2 r$
	$\leftarrow R_2, s_2$	
$r \leftarrow (R_1 + R_2).x \bmod q$		
$s_1 \leftarrow k_1 e + d_1 r$		
$s \leftarrow s_1 + s_2$		
	$s_1 \rightarrow$	
		$s \leftarrow s_1 + s_2$
return (r, s)		return (r, s)

Design rationale: the signing protocol

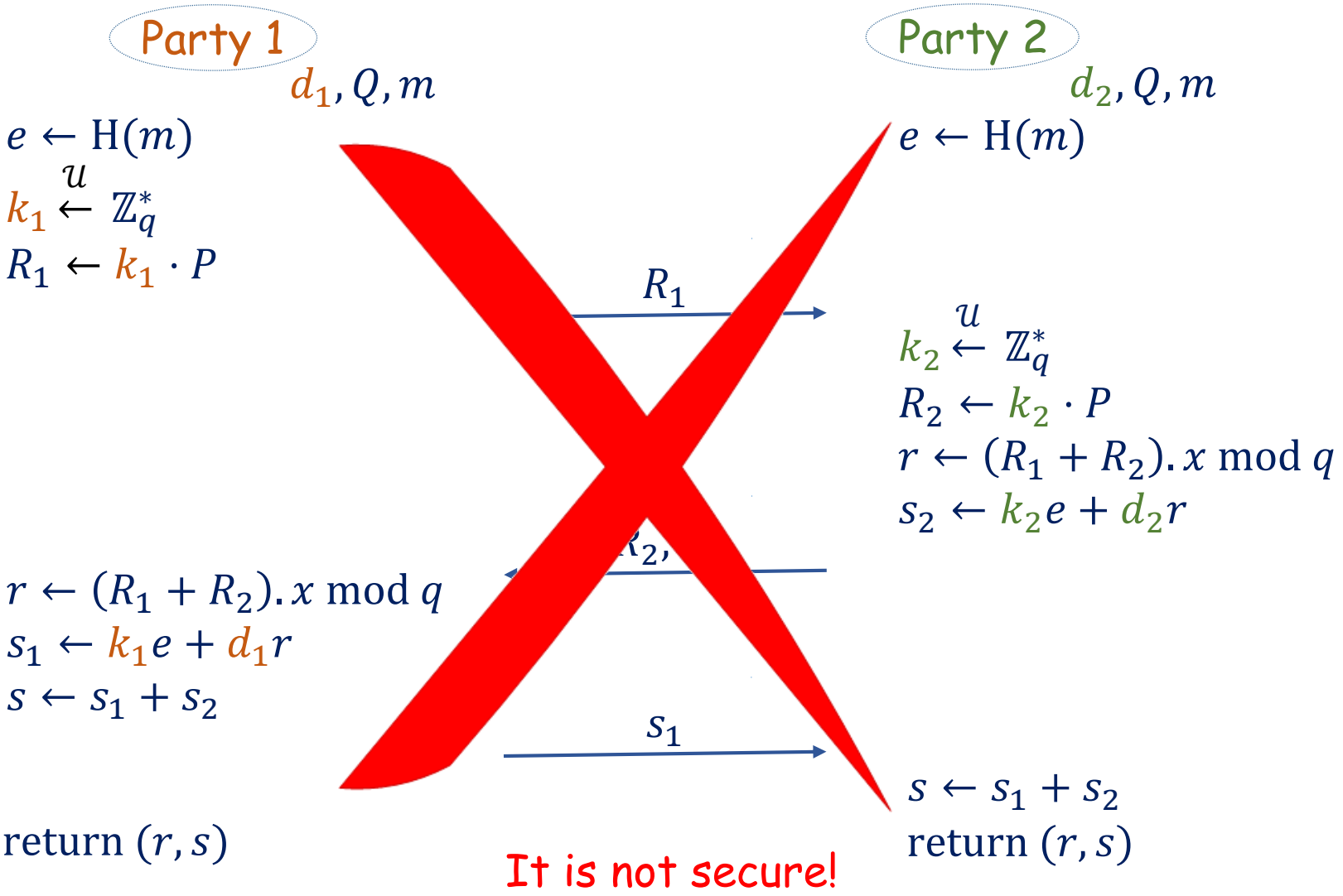
The naive version of the signing protocol:

Party 1		Party 2
d_1, Q, m		d_2, Q, m
$e \leftarrow \mathrm{H}(m)$		$e \leftarrow \mathrm{H}(m)$
$k_1 \overset{u}{\leftarrow} \mathbb{Z}_q^*$		
$R_1 \leftarrow k_1 \cdot P$		
	$R_1 \rightarrow$	
		$k_2 \overset{u}{\leftarrow} \mathbb{Z}_q^*$
		$R_2 \leftarrow k_2 \cdot P$
		$r \leftarrow (R_1 + R_2).x \bmod q$
		$s_2 \leftarrow k_2 e + d_2 r$
	$\leftarrow R_2, s_2$	
$r \leftarrow (R_1 + R_2).x \bmod q$		
$s_1 \leftarrow k_1 e + d_1 r$		
$s \leftarrow s_1 + s_2$		
	$s_1 \rightarrow$	
		$s \leftarrow s_1 + s_2$
return (r, s)		return (r, s)

Seems to be secure

Design rationale: the signing protocol

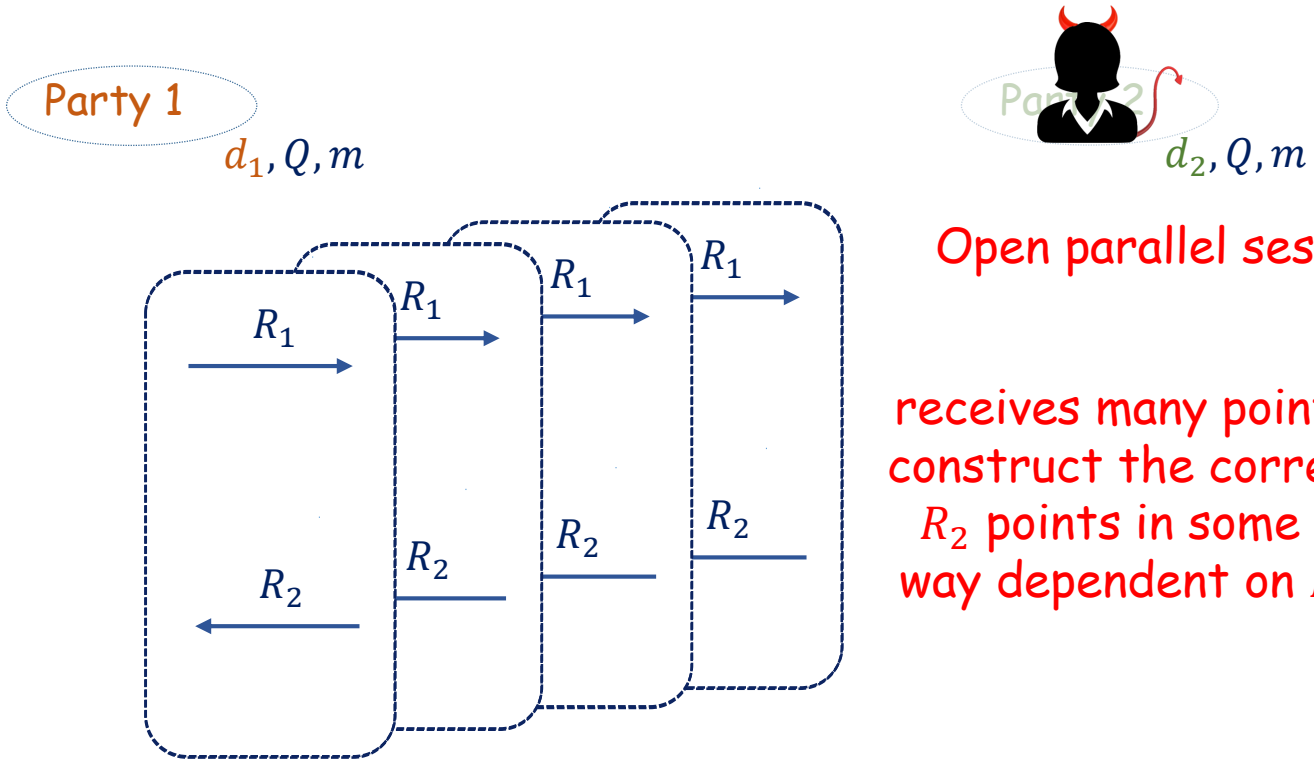
The naive version of the signing protocol:



Design rationale: the signing protocol

ROS-style attack [3], conditions:

- parallel sessions
- one party can select its parameters when it knows the parameters selected by the other party



Open parallel session

receives many points R_1 and construct the corresponding R_2 points in some specific way dependent on R_1 values

[3] Benhamouda, Fabrice and Lepoint, Tancr`ede and Loss, Julian and Orr`u, Michele and Raykova, Mariana, "On the (in) security of ROS", Journal of Cryptology, 35:4 (2022), 25

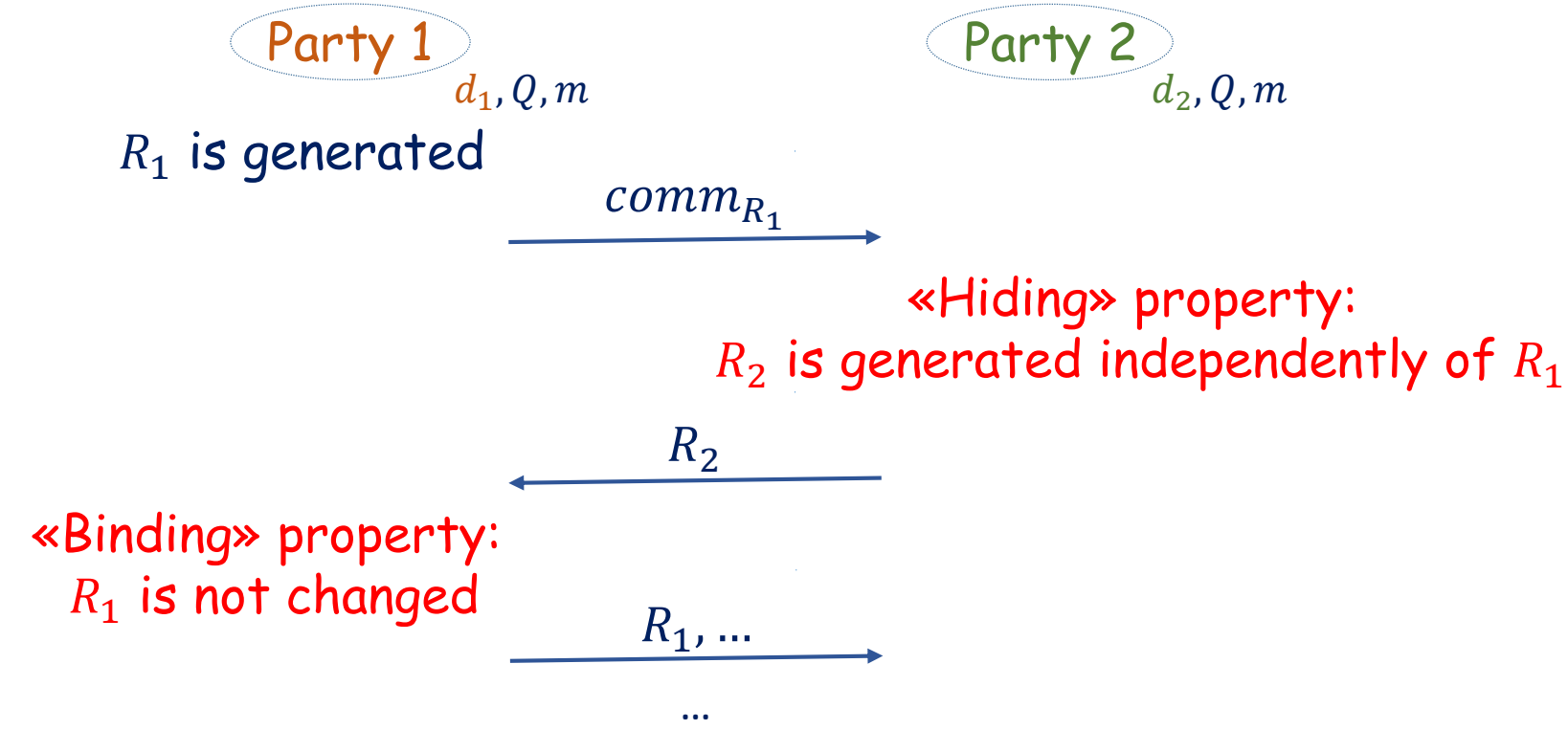
Search: the signing protocol

X	2010	N.A. Moldovyan	«Theoretical minimum and digital signature algorithms»
X	2010	Dzhunkovsky P. O., Ditenkova A. S.	«Threshold scheme of a digital signature with a shared secret based on GOST R 34.10-2001»
X	2011	S. Kim, J. Kim, J. Cheon,	«Threshold signature schemes for
X	2016	Epishkina, O. Isupova, K. Kogos, M. Shimkiv	nemes based on GOST R 34.10-2012»
XX	2020	Y. Zhang, M. Luo, K. Choo, L. Li, D. He	«Efficient and Secure Two-Party Distributed Signing Protocol for the GOST Signature Algorithm»
X	2022	T. N. Kim, D.H. Ngoc, N. A. Moldovyan	«New Collective Signatures Based on the Elliptic Curve Discrete Logarithm Problem»

ROS-style attack

Design rationale: the signing protocol

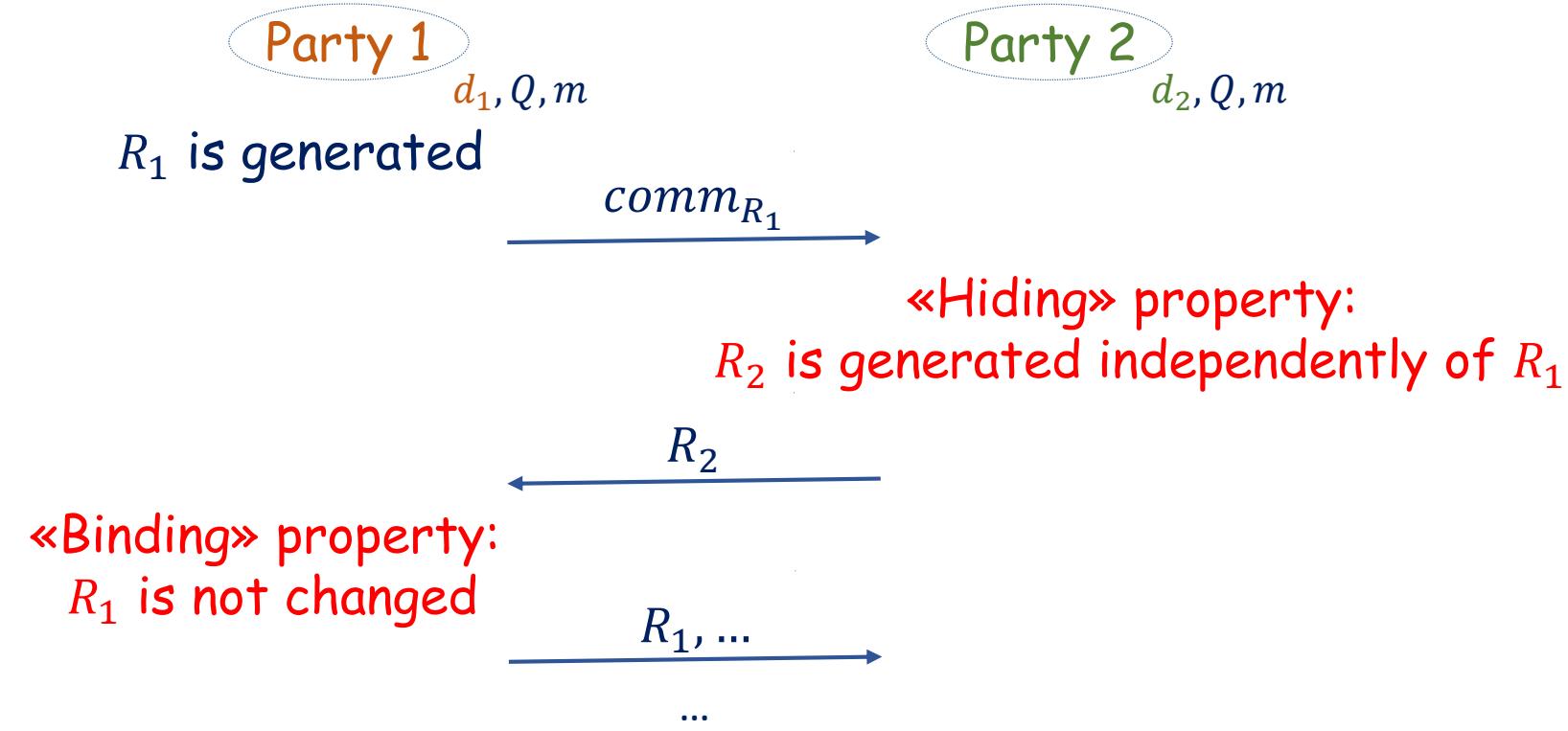
The commitment scheme is used to protect against this attack [1].



[1] Nicolosi, Antonio and Krohn, Maxwell N and Dodis, Yevgeniy and Mazieres, David, "Proactive Two-Party Signatures for User Authentication,", NDSS, 2003.

Design rationale: the signing protocol

The commitment scheme is used to protect against this attack [1].



*Each party should fix the message m before it learns the parameters of the other party to protect against the ROS-style attack

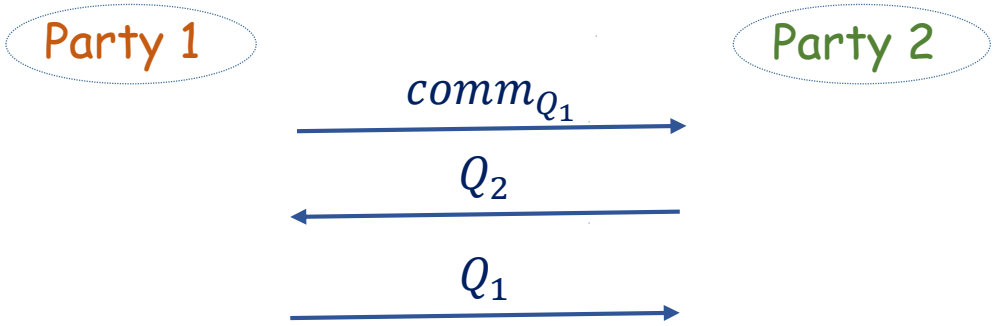
[1] Nicolosi, Antonio and Krohn, Maxwell N and Dodis, Yevgeniy and Mazieres, David, "Proactive Two-Party Signatures for User Authentication,", NDSS, 2003.

Search: the signing protocol

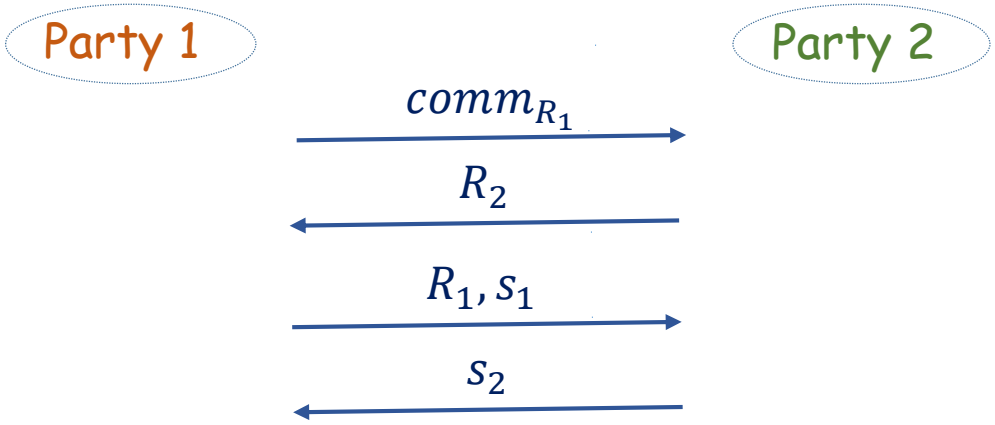
X	2010	N.A. Moldovyan	«Theoretical minimum and digital signature algorithms»
X	2010	Dzhunkovsky P. O., Ditenkova A. S.	«Threshold scheme of a digital signature with a shared secret based on GOST R 34.10-2001»
X	2011	S. Kim, J. Kim, J. Cheon, S. Ju	«Threshold signature schemes for ElGamal variants»
X	2016	A. Beresneva, A. Epishkina, O. Isupova, K. Kogos, M. Shimkiv	«Special digital signature schemes based on GOST R 34.10-2012»
X	2020	Y. Zhang, M. Luo, K. Choo, L. Li, D. He	«Efficient and Secure Two-Party Distributed Signing Protocol for the GOST Signature Algorithm»
X	2022	T. N. Kim, D.H. Ngoc, N. A. Moldovyan	«New Collective Signatures Based on the Elliptic Curve Discrete Logarithm Problem»

Synthesis: the 2p-GOST signature scheme

Key generation protocol of the 2p-GOST:



Signing protocol of the 2p-GOST:



Synthesis: the 2p-GOST signature scheme

KGen

$\mathbf{P_1}$ ( )		$\mathbf{P_2}$ ( )
$d_1 \xleftarrow{u} \mathbb{Z}_q^*$		
$Q_1 \leftarrow d_1 \cdot P$		
$(op_Q, comm_Q) \leftarrow \mathsf{Cmt}(Q_1)$		
	$\xrightarrow{comm_Q}$	
		$d_2 \xleftarrow{u} \mathbb{Z}_q^*$
		$Q_2 \leftarrow d_2 \cdot P$
	$\xleftarrow{Q_2}$	
if $(Q_2 = -Q_1)$: **return** $\perp$		
$Q \leftarrow Q_1 + Q_2$		
	$\xrightarrow{op_Q, Q_1}$	
		if $(\mathsf{Open}(comm_Q, Q_1, op_Q) = 0)$: **return** $\perp$
		if $(Q_1 = -Q_2)$: **return** $\perp$
		$Q \leftarrow Q_1 + Q_2$
return (d_1, Q)		**return** (d_2, Q)

Figure 5: Key generation protocol of the 2p-GOST signature scheme.

Sign

$\mathbf{P_1}$ (d_1, Q, m)		$\mathbf{P_2}$ (d_2, Q, m)
$k_1 \xleftarrow{u} \mathbb{Z}_q^*$		
$R_1 \leftarrow k_1 \cdot P$		
$(op_R, comm_R) \leftarrow \mathsf{Cmt}(R_1)$		
	$\xrightarrow{comm_R}$	
		$k_2 \xleftarrow{u} \mathbb{Z}_q^*$
		$R_2 \leftarrow k_2 \cdot P$
	$\xleftarrow{R_2}$	
if $(R_2 = -R_1)$: **return** $\perp$		
$r \leftarrow (R_1 + R_2).x \mod q$		
if $(r = 0)$: **return** $\perp$		
$e \leftarrow \mathrm{H}(m)$		
if $(e = 0)$: $e \leftarrow 1$		
$s_1 \leftarrow k_1 \cdot e + d_1 \cdot r$		
	$\xrightarrow{op_R, R_1, s_1}$	
		if $(\mathsf{Open}(comm_R, R_1, op_R) = 0)$: **return** $\perp$
		if $(R_1 = -R_2)$: **return** $\perp$
		$e \leftarrow \mathrm{H}(m)$
		if $(e = 0)$: $e \leftarrow 1$
		$r \leftarrow (R_1 + R_2).x \mod q$
		$s_2 \leftarrow k_2 \cdot e + d_2 \cdot r$
		$s \leftarrow s_1 + s_2$
		$\sigma \leftarrow (r, s)$
		if $(\mathsf{Verify}(Q, m, \sigma) = 0)$: **return** $\perp$
	$\xleftarrow{s_2}$	
$s \leftarrow s_1 + s_2$		
$\sigma \leftarrow (r, s)$		
if $(\mathsf{Verify}(Q, m, \sigma) = 0)$: **return** $\perp$		
return σ		**return** σ

Figure 7: Signing protocol of the 2p-GOST signature scheme.

Thank you for your attention!

nikiforova@cryptopro.ru