Security of compositions with implicit certificate schemes

Daniel Brown, *Matthew J. Campagna*, Scott Vanstone

Certicom Research

24 August 2009

Outline

1. Outline
2. Implicit Certificates
3. OMC-certified ECDSA attack
4. ECQV Certificate Scheme
5. Passive Security of ECDSA-verified ECQV
6. Deployments and Standardization
7. Summary
8. References

Digital Postage Marks

- 'Bandwidth of the Paper Channel' (Berson)
  - Rendered with low-cost printer, read with high speed imaging.
  - Mail sorting and postal verification happens at 10 feet/second.
  - Envelope is sender's real-estate.
  - Holds about 100 bytes of data
  - Cryptographic verification should be done in 10ms
  - Evidence the secure dispensing of funds ($ 25B annually)
  - Need for a self-verifiable digital postage mark.

Optimal Mail Certificates

- OMCs were initially presented to be used in conjunction with ECPVS (a variant of Nyberg-Ruepell signatures) with partial message recovery, by Pintsov and Vanstone to solve the self-verifiable mail piece problem [7].

Size	Field	Purpose
1	Version	Identify indicia type
2	Vendor	Vendor identifier
2	Model	Model of meter
4	Serial No.	Serial serial number
5	RESERVED	Future Expansion[0]
3	Postage	Amount of postage
5	AR	Accumulating register
4	DR	Decrementing register
4	MC	Mail category
4	Date	Date of postage
4	Zip	Origin Zipcode
24	Sig	ECPVS Signature
4	Certificate No.	Certificate serial number
21	Pub	Public key reconstruction point
87	TOTAL	Total size of payload

Optimal Mail Certificates

- OMCs were initially presented to be used in conjunction with ECPVS (a variant of Nyberg-Ruepell signatures) with partial message recovery, by Pintsov and Vanstone to solve the self-verifiable mail piece problem [7].
- The OMC scheme was considered for generic use, including composition with ECDSA.
- Qu discovered a detectable forgery attack on OMCs with ECDSA.
- This attack has been expanded to an undetectable forgery.
- The OMC scheme was modified to be the ECQV scheme we use today, no known attacks on composition
- Show the attack that worked with OMC and ECDSA appears to fail for ECQV and ECDSA.

Optimal Mail Certificates

- OMCs were initially presented to be used in conjunction with ECPVS (a variant of Nyberg-Ruepell signatures) with partial message recovery, by Pintsov and Vanstone to solve the self-verifiable mail piece problem [7].
- The OMC scheme was considered for generic use, including composition with ECDSA.
- Qu discovered a detectable forgery attack on OMCs with ECDSA.
- This attack has been expanded to an undetectable forgery.
- The OMC scheme was modified to be the ECQV scheme we use today, no known attacks on composition
- Show the attack that worked with OMC and ECDSA appears to fail for ECQV and ECDSA.

Optimal Mail Certificates

- OMCs were initially presented to be used in conjunction with ECPVS (a variant of Nyberg-Ruepell signatures) with partial message recovery, by Pintsov and Vanstone to solve the self-verifiable mail piece problem [7].
- The OMC scheme was considered for generic use, including composition with ECDSA.
- Qu discovered a detectable forgery attack on OMCs with ECDSA.
- This attack has been expanded to an undetectable forgery.
- The OMC scheme was modified to be the ECQV scheme we use today, no known attacks on composition
- Show the attack that worked with OMC and ECDSA appears to fail for ECQV and ECDSA.

Optimal Mail Certificates

- OMCs were initially presented to be used in conjunction with ECPVS (a variant of Nyberg-Ruepell signatures) with partial message recovery, by Pintsov and Vanstone to solve the self-verifiable mail piece problem [7].
- The OMC scheme was considered for generic use, including composition with ECDSA.
- Qu discovered a detectable forgery attack on OMCs with ECDSA.
- This attack has been expanded to an undetectable forgery.
- The OMC scheme was modified to be the ECQV scheme we use today, no known attacks on composition
- Show the attack that worked with OMC and ECDSA appears to fail for ECQV and ECDSA.

Optimal Mail Certificates

- OMCs were initially presented to be used in conjunction with ECPVS (a variant of Nyberg-Ruepell signatures) with partial message recovery, by Pintsov and Vanstone to solve the self-verifiable mail piece problem [7].
- The OMC scheme was considered for generic use, including composition with ECDSA.
- Qu discovered a detectable forgery attack on OMCs with ECDSA.
- This attack has been expanded to an undetectable forgery.
- The OMC scheme was modified to be the ECQV scheme we use today, no known attacks on composition
- Show the attack that worked with OMC and ECDSA appears to fail for ECQV and ECDSA.

Certificates

Definition (Traditional Certificate)

A traditional certificate binds a public key and user identity by affixing a digital signature to the structure. We can generalize a traditional certificate by a triple (I, P, sig).

Definition (Implicit Certificate)

An implicit certificate consists of an identity element I and public key reconstruction data P, which together with a CA public key can be used to reconstruct the identified entity's public key. We represent this as the pair (I, P).

Girault defined these constructions as self-certified public keys [4].
A security model for implicit certificates is given by Brown, Gallant, and Vanstone [3].

Optimal Mail Certificates

Definition (Optimal Mail Certificates)

Assume we have a CA with key pair (c, C).

- Certificate Request: Bob generates an ephemeral key pair (r, R) and sends R along with identity information to the CA.
- CA Transformation:
  - Define identity I for Bob.
  - Generate *public key reconstruction data* $P = R + kG$.
  - Compute *private key contribution data* $s = k + H(I, P)c \pmod{n}$
  - Return optimal mail certificate (I, P), and s
- Requestor Transformation: Bob computes private key $b = r + s \pmod{n}$

Optimal Mail Certificates

Definition (Optimal Mail Certificates)

Assume we have a CA with key pair (c, C).

- Certificate Request: Bob generates an ephemeral key pair (r, R) and sends R along with identity information to the CA.
- CA Transformation:
  - Define identity I for Bob.
  - Generate *public key reconstruction data* $P = R + kG$.
  - Compute *private key contribution data* $s = k + H(I, P)c \pmod{n}$
  - Return optimal mail certificate (I, P), and s
- Requestor Transformation: Bob computes private key $b = r + s \pmod{n}$

Optimal Mail Certificates

Definition (Optimal Mail Certificates)

Assume we have a CA with key pair (c, C).

- Certificate Request: Bob generates an ephemeral key pair (r, R) and sends R along with identity information to the CA.
- CA Transformation:
  - Define identity I for Bob.
  - Generate *public key reconstruction data* $P = R + kG$.
  - Compute *private key contribution data* $s = k + H(I, P)c \pmod{n}$
  - Return optimal mail certificate (I, P), and s
- Requestor Transformation: Bob computes private key $b = r + s \pmod{n}$

Optimal Mail Certificates

Recovering the public key

- Alice obtains Bob's implicit certificate (I, P).
- Alice computes Bob's public key $B = P + H(I, P)C$

The correctness of this can be seen in that

$$\begin{aligned} B &= P + H(I, P)C \\ &= R + kG + H(I, P)cG \\ &= rG + (k + H(I, P)c)G \\ &= (r + s)G. \end{aligned}$$

ECDSA

We will assume Bob, with key pair (b, B), is the signer of message M.

- Compute ephemeral key pair (t, T).
- Computes integer $u = \phi(T)$, by interpreting the x-coordinate of T as an integer modulo n.
- Compute $v = t^{-1}(H(M) + ub) \pmod{n}$.
- Publish (u, v) as Bob's signature on message M.

ECDSA

Alice can verify Bob's signature (u, v) on message M.

- Compute $w = v^{-1} \pmod{n}$.
- Compute $W = w(H(M)G + uB)$.
- Derive $y = \phi(W)$ an integer modulo n.
- Accept signature if $y = u$, else reject.

ECDSA

The correctness can be see by

$$
\begin{aligned}
W &= w(H(M)G + uB) \\
&= v^{-1}(H(M)G + ubG) \\
&= ((t^{-1}(H(M) + ub))^{-1}(H(M) + ub)G \\
&= tG \\
&= T
\end{aligned}
$$

Initial Attack

- The attacker Eve with access to the CA key, C, chooses a message M and identity I generates an implicit certificate (I, P), and signature (u, v) on M.
- ECDSA is not considered universally composable.
- The attack is not known to extend to ECPVS (originally proposed to be used with OMC).
- The attack is not known to extend to ECQV with ECDSA.

Qu's Attack

Definition (Qu's Attack)

Select random integer $f \in (0, n)$ and compute

$$u = \phi(fC),$$

$$P = -\frac{H(M)}{u} G,$$

and

$$v = \frac{uH(I, P)}{f} \pmod{n}.$$

Publish (I, P) and (u, v) as a implicit certificate for I and signature on message M.

Qu's Attack

To see that (I, P) and (u, v) is a valid implicit certificate and signature for message M note that,

$$B = P + H(I, P)C = -\frac{H(M)}{u}G + H(I, P)C$$

and next substitute this into the ECDSA verification equations we get

$$\begin{aligned} W &= v^{-1}\left(H(M)G + uB\right) \\ &= \left(\frac{uH(I, P)}{f}\right)^{-1}\left(H(M)G + uB\right) \end{aligned}$$

Qu's Attack

To see that (I, P) and (u, v) is a valid implicit certificate and signature for message M note that,

$$B = P + H(I, P)C = -\frac{H(M)}{u}G + H(I, P)C$$

and next substitute this into the ECDSA verification equations we get

$$\begin{aligned} W &= v^{-1}\left(H(M)G + uB\right) \\ &= \left(\frac{f}{uH(I, P)}\right)\left(H(M)G + uB\right) \end{aligned}$$

Qu's Attack

To see that (I, P) and (u, v) is a valid implicit certificate and signature for message M note that,

$$B = P + H(I, P)C = -\frac{H(M)}{u}G + H(I, P)C$$

and next substitute this into the ECDSA verification equations we get

$$\begin{aligned} W &= v^{-1}\left(H(M)G + uB\right) \\ &= \left(\frac{f}{uH(I, P)}\right)\left(H(M)G + u\left(-\frac{H(M)}{u}G + H(I, P)C\right)\right) \end{aligned}$$

Qu's Attack

To see that (I, P) and (u, v) is a valid implicit certificate and signature for message M note that,

$$B = P + H(I, P)C = -\frac{H(M)}{u}G + H(I, P)C$$

and next substitute this into the ECDSA verification equations we get

$$\begin{aligned} W &= v^{-1}\left(H(M)G + uB\right) \\ &= \left(\frac{f}{uH(I, P)}\right)\left(H(M)G + u\left(-\frac{H(M)}{u}G + H(I, P)C\right)\right) \\ &= \frac{f}{uH(I, P)}\left(H(M)G - H(M)G + uH(I, P)C\right) \end{aligned}$$

Qu's Attack

To see that (I, P) and (u, v) is a valid implicit certificate and signature for message M note that,

$$B = P + H(I, P)C = -\frac{H(M)}{u}G + H(I, P)C$$

and next substitute this into the ECDSA verification equations we get

$$\begin{aligned} W &= v^{-1}\left(H(M)G + uB\right) \\ &= \left(\frac{f}{uH(I, P)}\right)\left(H(M)G + u\left(-\frac{H(M)}{u}G + H(I, P)C\right)\right) \\ &= \frac{f}{uH(I, P)}\left(uH(I, P)C\right) \end{aligned}$$

Qu's Attack

To see that (I, P) and (u, v) is a valid implicit certificate and signature for message M note that,

$$B = P + H(I, P)C = -\frac{H(M)}{u}G + H(I, P)C$$

and next substitute this into the ECDSA verification equations we get

$$\begin{aligned} W &= v^{-1}\left(H(M)G + uB\right) \\ &= \left(\frac{f}{uH(I,P)}\right)\left(H(M)G + u\left(-\frac{H(M)}{u}G + H(I,P)C\right)\right) \\ &= \frac{f}{uH(I,P)}\left(uH(I,P)C\right) \\ &= fC. \end{aligned}$$

Qu's Attack

This is a detectable forgery.
Given a certificate (I, P) and a signed message M, (u, v) we can check

$$P = -\frac{H(M)}{u} G$$

If the above is true, then the signature can be assumed forged.

Qu's Attack

The associated private key is not known to Eve. Note that

$$b = -\frac{H(M)}{u} + H(I, P)c \pmod{n}$$

and if Eve knows the private key, then Eve can solve for c.

The definition of security given by Brown, Gallant and Vanstone [3] is based on an adversary being able to create a certificate for which the private key is known.

Generalized Attack

This is accomplished by an attacker Eve with access to the CA's public key C, to choose message M, identity I, and $0 < d, f < n$ and compute (P, u, v);

$$u = \phi(fC),$$

$$P = dC - \frac{H(M)}{u} G$$

and,

$$v = \frac{u(d + H(I, P))}{f} \pmod{n}.$$

Generalized Attack

To see the (I, P) and (u, v) is a valid implicit certificate and signature for message M note that,

$$B = P + H(I, P)C = dC - \frac{H(M)}{u}G + H(I, P)C$$

and next substitute this into the ECDSA verification equations we get

$$\begin{aligned} W &= v^{-1}(H(M)G + uB) \\ &= \left(\frac{u(d + H(I, P))}{f}\right)^{-1}(H(M)G + uB) \end{aligned}$$

Generalized Attack

To see the (I, P) and (u, v) is a valid implicit certificate and signature for message M note that,

$$B = P + H(I, P)C = dC - \frac{H(M)}{u}G + H(I, P)C$$

and next substitute this into the ECDSA verification equations we get

$$\begin{aligned} W &= v^{-1}(H(M)G + uB) \\ &= \left(\frac{f}{u(d + H(I, P))}\right)(H(M)G + uB) \end{aligned}$$

Generalized Attack

To see the (I, P) and (u, v) is a valid implicit certificate and signature for message M note that,

$$B = P + H(I, P)C = dC - \frac{H(M)}{u}G + H(I, P)C$$

and next substitute this into the ECDSA verification equations we get

$$\begin{aligned} W &= v^{-1}(H(M)G + uB) \\ &= \left(\frac{f}{u(d + H(I, P))}\right)\left(H(M)G + u\left(dC - \frac{H(M)}{u}G + H(I, P)C\right)\right) \end{aligned}$$

Generalized Attack

To see the (I, P) and (u, v) is a valid implicit certificate and signature for message M note that,

$$B = P + H(I, P)C = dC - \frac{H(M)}{u}G + H(I, P)C$$

and next substitute this into the ECDSA verification equations we get

$$\begin{aligned} W &= v^{-1}(H(M)G + uB) \\ &= \left(\frac{f}{u(d + H(I, P))}\right)\left(H(M)G + u\left(dC - \frac{H(M)}{u}G + H(I, P)C\right)\right) \\ &= \left(\frac{f}{u(d + H(I, P))}\right)(H(M)G + udC - H(M)G + uH(I, P)C) \end{aligned}$$

Generalized Attack

To see the (I, P) and (u, v) is a valid implicit certificate and signature for message M note that,

$$B = P + H(I, P)C = dC - \frac{H(M)}{u}G + H(I, P)C$$

and next substitute this into the ECDSA verification equations we get

$$\begin{aligned} W &= v^{-1}(H(M)G + uB) \\ &= \left(\frac{f}{u(d + H(I, P))}\right)\left(H(M)G + u\left(dC - \frac{H(M)}{u}G + H(I, P)C\right)\right) \\ &= \left(\frac{f}{u(d + H(I, P))}\right) u(d + H(I, P))C \end{aligned}$$

Generalized Attack

To see the (I, P) and (u, v) is a valid implicit certificate and signature for message M note that,

$$B = P + H(I, P)C = dC - \frac{H(M)}{u}G + H(I, P)C$$

and next substitute this into the ECDSA verification equations we get

$$\begin{aligned} W &= v^{-1}(H(M)G + uB) \\ &= \left(\frac{f}{u(d + H(I, P))}\right)\left(H(M)G + u\left(dC - \frac{H(M)}{u}G + H(I, P)C\right)\right) \\ &= \left(\frac{f}{u(d + H(I, P))}\right)u(d + H(I, P))C \\ &= fC. \end{aligned}$$

Undetectable Forgery

To see this is an undetectable forgery, suppose we have an authentic certificate (I, P) and signature (u, v) on a message M.

	Legitimate Signature	Possible Forger
u	$u = \phi(tG)$	
P	$P = rG + kG$	
v	$W = v^{-1}(H(M)G + uB)$	

Any legitimate signature is indistinguishable from a forgery. However, every forged signature requires a new certificate.

Undetectable Forgery

To see this is an undetectable forgery, suppose we have an authentic certificate (I, P) and signature (u, v) on a message M.

	Legitimate Signature	Possible Forger
u	$u = \phi(tG)$	$u = \phi(tG) = \phi(fC)$ for some f
P	$P = rG + kG$	
v	$W = v^{-1}(H(M)G + uB)$	

Any legitimate signature is indistinguishable from a forgery. However, every forged signature requires a new certificate.

Undetectable Forgery

To see this is an undetectable forgery, suppose we have an authentic certificate (I, P) and signature (u, v) on a message M.

	Legitimate Signature	Possible Forger
u	$u = \phi(tG)$	$u = \phi(tG) = \phi(fC)$ for some f
P	$P = rG + kG$	$P = dC - \frac{H(M)}{u}G$ for some d
v	$W = v^{-1}(H(M)G + uB)$	

Any legitimate signature is indistinguishable from a forgery. However, every forged signature requires a new certificate.

Undetectable Forgery

To see this is an undetectable forgery, suppose we have an authentic certificate (I, P) and signature (u, v) on a message M.

	Legitimate Signature	Possible Forger
u	$u = \phi(tG)$	$u = \phi(tG) = \phi(fC)$ for some f
P	$P = rG + kG$	$P = dC - \frac{H(M)}{u}G$ for some d
v	$vW = H(M)G + uB$	

Any legitimate signature is indistinguishable from a forgery. However, every forged signature requires a new certificate.

Undetectable Forgery

To see this is an undetectable forgery, suppose we have an authentic certificate (I, P) and signature (u, v) on a message M.

	Legitimate Signature	Possible Forger
u	$u = \phi(tG)$	$u = \phi(tG) = \phi(fC)$ for some f
P	$P = rG + kG$	$P = dC - \frac{H(M)}{u}G$ for some d
v	$vW = H(M)G + uB$	v is completely determined.

Any legitimate signature is indistinguishable from a forgery. However, every forged signature requires a new certificate.

Undetectable Forgery

To see this is an undetectable forgery, suppose we have an authentic certificate (I, P) and signature (u, v) on a message M.

	Legitimate Signature	Possible Forger
u	$u = \phi(tG)$	$u = \phi(tG) = \phi(fC)$ for some f
P	$P = rG + kG$	$P = dC - \frac{H(M)}{u}G$ for some d
v	$vW = H(M)G + uB$	v is completely determined.

Any legitimate signature is indistinguishable from a forgery.
However, every forged signature requires a new certificate.

Undetectable Forgery

To see this is an undetectable forgery, suppose we have an authentic certificate (I, P) and signature (u, v) on a message M.

	Legitimate Signature	Possible Forger
u	$u = \phi(tG)$	$u = \phi(tG) = \phi(fC)$ for some f
P	$P = rG + kG$	$P = dC - \frac{H(M)}{u}G$ for some d
v	$vW = H(M)G + uB$	v is completely determined.

Any legitimate signature is indistinguishable from a forgery. However, every forged signature requires a new certificate.

OMC-verified ECDSA Analysis

To see this attack does not seem to work for ECQV-verified ECDSA it is worth stepping through some of the analysis on the OMC-verified ECDSA. Starting with the ECDSA verification equation

$$W = v^{-1}(H(M)G + uB)$$

and substituting in for $B = P + H(I, P)C$

$$vW = H(M)G + uP + uH(I, P)C$$

OMC-verified ECDSA Analysis

Starting with,

$$vW = H(M)G + uP + uH(I, P)C$$

we can simplify notation $h = H(M)$ and $q = H(I, P)$ and re-write the above as

$$vW - uP = hG + quC.$$

which can be written in matrix format

$$\begin{pmatrix} -u & v \end{pmatrix} \begin{pmatrix} P \\ W \end{pmatrix} = \begin{pmatrix} qu & h \end{pmatrix} \begin{pmatrix} C \\ G \end{pmatrix}$$

OMC-verified ECDSA Analysis

For some integers d, e, f, g we have

$$\begin{pmatrix} P \\ W \end{pmatrix} = \begin{pmatrix} d & e \\ f & g \end{pmatrix} \begin{pmatrix} C \\ G \end{pmatrix},$$

and re-express the prior matrix equation dropping the points and get

$$\begin{pmatrix} -u & v \end{pmatrix} \begin{pmatrix} P \\ W \end{pmatrix} = \begin{pmatrix} qu & h \end{pmatrix} \begin{pmatrix} C \\ G \end{pmatrix}$$

OMC-verified ECDSA Analysis

For some integers d, e, f, g we have

$$\begin{pmatrix} P \\ W \end{pmatrix} = \begin{pmatrix} d & e \\ f & g \end{pmatrix} \begin{pmatrix} C \\ G \end{pmatrix},$$

and re-express the prior matrix equation dropping the points and get

$$\begin{pmatrix} P & W \end{pmatrix} \begin{pmatrix} -u \\ v \end{pmatrix} = \begin{pmatrix} C & G \end{pmatrix} \begin{pmatrix} qu \\ h \end{pmatrix}$$

OMC-verified ECDSA Analysis

For some integers d, e, f, g we have

$$\begin{pmatrix} P \\ W \end{pmatrix} = \begin{pmatrix} d & e \\ f & g \end{pmatrix} \begin{pmatrix} C \\ G \end{pmatrix},$$

and re-express the prior matrix equation dropping the points and get

$$\begin{pmatrix} d & f \\ e & g \end{pmatrix} \begin{pmatrix} -u \\ v \end{pmatrix} = \begin{pmatrix} qu \\ h \end{pmatrix}.$$

OMC-verified ECDSA Analysis

For some integers d, e, f, g we have

$$\begin{pmatrix} P \\ W \end{pmatrix} = \begin{pmatrix} d & e \\ f & g \end{pmatrix} \begin{pmatrix} C \\ G \end{pmatrix},$$

and re-express the prior matrix equation dropping the points and get

$$\begin{pmatrix} d & f \\ e & g \end{pmatrix} \begin{pmatrix} -u \\ v \end{pmatrix} = \begin{pmatrix} qu \\ h \end{pmatrix}.$$

A successful forgery needs to solve for the matrix $\left(\begin{smallmatrix} d & f \\ e & g \end{smallmatrix}\right)$ and the free variable v.

$$\begin{pmatrix} -u \\ v \end{pmatrix} = \frac{1}{dg - ef} \begin{pmatrix} gqu - fh \\ -equ + dh \end{pmatrix}$$

OMC-verified ECDSA Analysis

The matrix equation

$$\begin{pmatrix} -u \\ v \end{pmatrix} = \frac{1}{dg - ef} \begin{pmatrix} gqu - fh \\ -equ + dh \end{pmatrix}$$

gives us two equations and five unknowns. We can remove the non-linear property introduced by $q = H(I, P)$, by selecting $g = 0$, to solve for

$$-u = \frac{gqu - fh}{dg - ef}$$

$$e = -\frac{h}{u} = -\frac{H(M)}{\phi(fC)}$$

So, for $g = 0$ and any value f we can solve for e.

OMC-verified ECDSA Analysis

The matrix equation

$$\begin{pmatrix} -u \\ v \end{pmatrix} = \frac{1}{dg - ef} \begin{pmatrix} gqu - fh \\ -equ + dh \end{pmatrix}$$

gives us two equations and five unknowns. We can remove the non-linear property introduced by $q = H(I, P)$, by selecting $g = 0$, to solve for

$$-u = \frac{-fh}{-ef}$$

$$e = -\frac{h}{u} = -\frac{H(M)}{\phi(fC)}$$

So, for $g = 0$ and any value f we can solve for e.

OMC-verified ECDSA Analysis

The matrix equation

$$\begin{pmatrix} -u \\ v \end{pmatrix} = \frac{1}{dg - ef} \begin{pmatrix} gqu - fh \\ -equ + dh \end{pmatrix}$$

gives us two equations and five unknowns. We can remove the non-linear property introduced by $q = H(I, P)$, by selecting $g = 0$, to solve for

$$-u = \frac{h}{e}$$

$$e = -\frac{h}{u} = -\frac{H(M)}{\phi(fC)}$$

So, for $g = 0$ and any value f we can solve for e.

OMC-verified ECDSA Analysis

We can re-express the matrix with $g = 0$,

$$\begin{pmatrix} -u \\ v \end{pmatrix} = \frac{1}{ef} \begin{pmatrix} fh \\ equ - dh \end{pmatrix}$$

Now for any d, f value we have

$$v = \frac{equ - dh}{ef} = \frac{-\frac{h}{u}qu - dh}{-\frac{h}{u}f} = \frac{u(d+q)}{f}.$$

This allows the previous description of the undetectable forgery,

$$u = \phi(fC),$$

$$P = dC + eG = dC - \frac{H(M)}{\phi(fC)}G$$

and,

$$v = \frac{u(d + H(I, P))}{f} \pmod{n}.$$

ECQV

ECQV was modified to protect against this composition attack.

Definition (ECQV)

- Certificate Request: Bob generates an ephemeral key pair (r, R) and sends R along with identity information to the CA.
- CA Transformation:
  - Define identity I for Bob.
  - Generate *public key reconstruction data* $P = R + kG$.
  - Compute *private key contribution data* $s = c + H(I, P)k \pmod{n}$
  - Return implicit certificate (I, P), and s
- Requestor Transformation: Bob computes private key $b = s + H(I, P)r \pmod{n}$

ECQV

Recovering the public key

- Alice obtains Bob's implicit certificate (I, P).
- Alice computes Bob's public key $B = C + H(I, P)P$

The correctness of this can be seen in that

$$\begin{aligned} B &= C + H(I,P)P \\ &= cG + H(I,P)(R + kG) \\ &= cG + H(I,P)(r + k)G \\ &= (c + H(I,P)k + H(I,P)rG. \\ &= (s + H(I,P)r)G \end{aligned}$$

Attempting forgeries on ECQV-verified ECDSA

	OMC	ECQV
CA Key	$C = cG$	$C = cG$
Request	$R = rG$	$R = rG$
Implicit cert	$P = R + kG$	$P = R + kG$
Private rcstr.	$s = k + H(I, P)c$	$s = c + H(I, P)k$
Private key	$b = r + s$	$b = s + H(I, P)r$
Public key	$B = P + H(I, P)C$	$B = C + H(I, P)P$

Table: Comparison of the OMC and ECQV

Attempting forgeries on ECQV-certified ECDSA

OMC and ECQV composed with ECDSA side-by-side.

OMC	ECQV
$q = H(I, dC + eG)$	$q = H(I, dC + eG)$
$u = \phi(fC + gG)$	$u = \phi(fC + gG)$
$\begin{pmatrix} -u \\ v \end{pmatrix} = \frac{1}{dg - ef} \begin{pmatrix} gqu - fh \\ -equ + dh \end{pmatrix}$	$\begin{pmatrix} -qu \\ v \end{pmatrix} = \frac{1}{dg - ef} \begin{pmatrix} gu - fh \\ -eu + dh \end{pmatrix}$

Here we found no way to isolate the non-linear effects of q and u to solve for e, f, g, and h.

Passive Security of ECDSA-verified ECQV

Theorem

There does not exist a passive adversary against ECDSA combined with ECQV that succeeds in the combined random oracle and generic group model.

ZigBee Smart Energy

ZigBee is a wireless mesh-networking standard based on low-power IEEE 802.15.4 standard for wireless personal area networking.

- Native packet size is 127-bytes.
  - Data payload from 96 - 112 bytes depending on mesh.
- Uses AES-CCM to secure network and peer-to-peer traffic.
- Low-powered devices typically no greater than 16-bit, 24Mhz

ZigBee Smart Energy profile requires authenticated key agreement to securely establish network and application keys.

- Every device is manufactured with an ECQV certificate.
- Performs an ECMQV key agreement to join the network and obtain application key.
- Signs demand-response messages issued from utilities.

Deployments and Standardization

- Standards
  - Standards for Efficient Cryptography Groups's SEC 4.
  - ZigBee Smart Energy Profile
  - ISA SP100.11a
  - CEN DPM Infrastructure Standard
- Deployments
  - ZigBee Smart Meters 1.5 Million
  - SMS and cellular modem messaging application
  - Self-verified digital postmarks

Summary & Further Work

Summary

- OMC with ECDSA is vulnerable to undetectable forgery attacks.
- ECQV with ECDSA is secure against passive adversary

Further Work

- Consideration against an active adversary
- Weaken the assumptions used in the security proof.
- Generalization of the security to other implicit certificate schemes and signature schemes or key agreement schemes.

Thank you for your attention

References

D. R. L. Brown. Generic groups, collision resistance, and ECDSA. *Designs, Codes and Cryptography*, 35:119–152, 2005.

D. R. L. Brown. On the provable security of ECDSA. In I. F. Blake, G. Seroussi, and N. P. Smart, editors, *Advances in Elliptic Curve Cryptography*, volume 317 of *London Mathematical Society Lecture Note Series*, pages 21–40. Cambridge University Press, 2005.

D. R. L. Brown, R. P. Gallant, and S. A. Vanstone. Provably secure implicit certificate schemes. In P. F. Syverson, editor, *Financial Cryptography — FC 2001*, volume 2339 of *Lecture Notes in Computer Science*, pages 156–165. Springer, Feb. 2001.

M. Girault. Self-certified public keys.D. Davies, editor, *Advances in Cryptology — EUROCRYPT 1991*, number 547 in LNCS pages 490-497. IACR, Springer, 1991.

C. G. Günther. An identity-based key-exchange protocol, *Advances in Cryptology —EUROCRYPT 1989*, pages 29–37, Springer, 1990.

P. Paillier and D. Vergnaud. Discrete-log-based signatures may not be equivalent to discrete log. In B. Roy, editor, *Advances in Cryptology — ASIACRYPT 2005*, number 3788 in LNCS, pages 1–20. IACR, Springer, Dec. 2005.

L. A. Pintsov and S. A. Vanstone. Postal revenue collection in the digital age. In Y. Frankel, editor, *Financial Cryptography — FC 2001*, volume 19622339 of *Lecture Notes in Computer Science*, pages 105–120. Springer, Feb. 2000.

M. Qu. Attack on ECDSA with original optimal mail certificates. Personal Communication, 2000.